

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Kil-ho SHIN, Yuzuru FUKUDA, Hironori
GOTOH

Application No.: New U.S. Patent Application

Filed: September 6, 2000

Docket No.: 107215

For: DATA STORAGE DEVICE PROVIDED WITH FUNCTION FOR USER'S ACCESS
RIGHT

CLAIM FOR PRIORITY

Director of the U.S. Patent and Trademark Office
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 11-293752 filed October 15, 1999

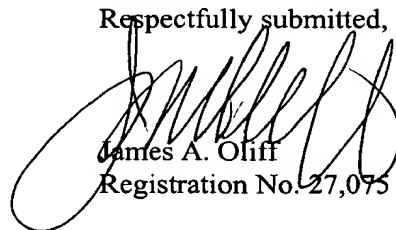
In support of this claim, a certified copy of said original foreign application:

 X is filed herewith.

 was filed on in Parent Application No. filed .

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,


James A. Oliff
Registration No. 27,075

Thomas J. Pardini
Registration No. 30,411

JAO:TJP/cmm
Date: September 6, 2000

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

<p>DEPOSIT ACCOUNT USE AUTHORIZATION Please grant any extension necessary for entry; Charge any fee due to our Deposit Account No. 15-0461</p>



日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

JPO853 U.S. PTO
09/656315
09/06/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1999年10月15日

出 願 番 号
Application Number:

平成11年特許願第293752号

出 願 人
Applicant(s):

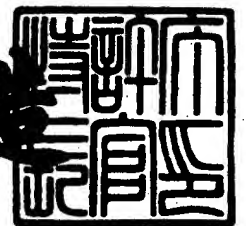
富士ゼロックス株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 7月21日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3056401

【書類名】 特許願

【整理番号】 FN99-00120

【提出日】 平成11年10月15日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/30

【発明の名称】 アクセス資格認証機能付きデータ記憶装置

【請求項の数】 52

【発明者】

【住所又は居所】 神奈川県足柄上郡中井町境 4 3 0 グリーンテクなかい
富士ゼロックス株式会社内

【氏名】 申 吉浩

【発明者】

【住所又は居所】 神奈川県足柄上郡中井町境 4 3 0 グリーンテクなかい
富士ゼロックス株式会社内

【氏名】 福田 譲

【発明者】

【住所又は居所】 神奈川県足柄上郡中井町境 4 3 0 グリーンテクなかい
富士ゼロックス株式会社内

【氏名】 後藤 広則

【特許出願人】

【識別番号】 000005496

【氏名又は名称】 富士ゼロックス株式会社

【電話番号】 0462-38-8516

【代理人】

【識別番号】 100086531

【弁理士】

【氏名又は名称】 澤田 俊夫

【電話番号】 03-5541-7577

【手数料の表示】

【予納台帳番号】 038818

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 アクセス資格認証機能付きデータ記憶装置

【特許請求の範囲】

【請求項 1】 アプリケーションプログラムによる記憶媒体中のデータへのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記アプリケーションプログラムのユーザのアクセス資格を認証するアクセス資格認証機能付きデータ記憶装置において、

認証用データを記憶する第 1 の記憶手段と、

アプリケーションプログラムのユーザの固有情報を記憶する第 2 の記憶手段と

、
上記アプリケーションプログラムのユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第 3 の記憶手段と、

上記第 1 の記憶手段に保持されている認証用データと、上記第 2 の記憶手段に記憶されている上記アプリケーションプログラムのユーザの固有情報と、上記第 3 の記憶手段に記憶されている上記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段と、

記録媒体を備えこの記録媒体にデータを記憶保存するデータ記憶装置本体と、

上記アプリケーションプログラムに設けられ、上記データ記憶装置本体の記録媒体に記憶されたデータに対する操作を指示するコマンドを生成するコマンド生成手段と、

上記アプリケーションプログラムに設けられ、上記コマンド生成手段によって生成されたコマンドを上記アプリケーションプログラムの外部に発行するコマンド発行手段と、

上記証明データ生成手段によって生成された証明データが上記アクセス資格認証の特徴情報に基づいて生成されていることを検証する証明データ検証手段と、

上記データ記憶装置本体のデータに対する操作を指示するコマンドのうちの少なくとも 1 種類のコマンドについては、上記検証が成功した場合に限り上記コマンドの実行を許容するコマンド管理手段とを有することを特徴とするアクセス資

格認証機能付きデータ記憶装置。

【請求項 2】 少なくとも、上記第 2 の記憶手段と、上記証明データ生成手段とが、内部のデータ及び処理手続を外部から観測することを困難ならしめる防御手段中に保持されていることを特徴とする請求項 1 記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 3】 少なくとも、上記第 2 の記憶手段と、上記証明データ生成手段とが、ＩＣカードなどの携帯可能な小型演算装置として構成されていることを特徴とする請求項 1 記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 4】 上記証明データ生成手段が、第 1 の演算手段と、第 2 の演算手段とから構成され、第 1 の演算手段は、上記第 2 の記憶手段に記憶されているアプリケーションプログラムのユーザの固有情報と、上記第 3 の記憶手段に記憶されている証明用補助情報とに所定の計算を施し、その結果として上記アクセス資格認証の特徴情報を算出し、第 2 の演算手段は、上記第 1 の記憶手段に記憶されている認証用データと、第 1 の演算手段によって算出されたアクセス資格認証の特徴情報とに所定の計算を施し、その結果として上記証明データを生成することを特徴とする請求項 1 乃至 3 記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 5】 上記証明データ生成手段が、第 3 の演算手段と、第 4 の演算手段と、第 5 の演算手段とから構成され、第 3 の演算手段は、上記第 1 の記憶手段に記憶されている認証用データと、上記第 3 の記憶手段に記憶されている証明用補助情報とに所定の計算を施し、第 4 の演算手段は、上記第 1 の記憶手段に記憶されている認証用データと、第 2 の記憶手段に記憶されているアプリケーションプログラムのユーザの固有情報とに所定の計算を施し、第 5 の演算手段が、上記第 3 の演算手段による計算結果と、上記第 4 の演算手段による計算結果とに所定の計算を施し、その結果として上記証明データを生成することを特徴とする請求項 1 乃至 3 記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 6】 少なくとも、上記第 2 の記憶手段と、上記第 4 の演算手段とが、内部のデータ及び処理手続を外部から観測することを困難ならしめる防御手段中に保持されていることを特徴とする請求項 5 に記載のアクセス資格認証機能

付きデータ記憶装置。

【請求項 7】 少なくとも、上記第 2 の記憶手段と、上記第 4 の演算手段とが、IC カードなどの携帯可能な小型演算装置として構成されていることを特徴とする請求項 5 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 8】 上記アクセス資格認証の特徴情報が暗号関数における復号鍵であり、上記認証用データが適当なデータを前記復号鍵に対応する暗号化鍵を用いて暗号化したものであり、上記証明データ検証手段は、上記証明データ生成手段が生成する上記証明データが認証用データを正しく復号したものであることを検証することを特徴とする請求項 1 乃至 7 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 9】 上記アクセス資格認証の特徴情報が暗号関数における暗号化鍵であり、上記証明データ生成手段が生成する上記証明データが上記認証用データを前記暗号化鍵を用いて正しく暗号化したものであることを検証することを特徴とする請求項 1 乃至 7 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 10】 上記アクセス資格認証の特徴情報がデジタル署名関数における署名鍵であり、上記証明データ生成手段が生成する上記証明データが、上記認証用データに対して、前記署名鍵を用いて正しく生成されたデジタル署名であることを検証することを特徴とする請求項 1 乃至 7 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 11】 暗号化関数が非対称鍵暗号関数であり、アクセス資格認証の特徴情報が鍵の一方であることを特徴とする請求項 8 または 9 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 12】 暗号化関数が公開鍵暗号関数であり、アクセス資格認証の特徴情報が秘密鍵であることを特徴とする請求項 11 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 13】 暗号化関数が対称鍵暗号関数であり、アクセス資格認証の特徴情報が共通秘密鍵であることを特徴とする請求項 8 または 9 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 14】 上記第 1 の記憶手段と、上記第 2 の記憶手段と、上記第 3

の記憶手段と、上記証明データ生成手段とから構成される証明データ生成装置と、上記証明データ検証手段に加え、認証用データを記憶する第4の記憶手段と、証明データを記憶する第5の記憶手段を備えた証明データ検証装置とが、互いに通信することによりアプリケーションプログラムのユーザのアクセス資格を認証するアクセス資格認証機能付きデータ記憶装置において、証明データ検証装置は、第4の記憶手段に記憶されている認証用データを証明データ生成装置の第1の記憶手段に書き出し証明データ生成装置は、証明データ生成手段によって第1の記憶手段に書き込まれた上記認証用データをもとに生成した証明データを、証明データ検証装置中の第5の記憶手段に書き出し、証明データ検証装置は第5の記憶手段に書き込まれた上記証明データを用いてアプリケーションプログラムのユーザのアクセス資格を認証することを特徴する請求項1乃至13に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項15】 上記アクセス資格認証の特徴情報が暗号化関数の暗号化鍵であり、証明データ検証装置が乱数生成手段を備え、乱数生成手段は生成した乱数を認証用データとして第4の記憶手段に書き込み、証明データ検証手段は、証明データ生成装置によって第5の記憶手段に書き込まれた証明データが前記乱数である認証用データをアクセス資格認証の特徴情報である暗号化鍵で暗号化したものであることを検証することを特徴とする請求項14に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項16】 アクセス資格認証の特徴情報が暗号化関数の復号鍵であり、証明データ検証装置が乱数生成手段と、生成した乱数を記憶する第6の記憶手段と、認証用素データを記憶する第7の記憶手段とを備え、乱数生成手段は生成した乱数を第6の記憶手段に書き込むと共に、第7の記憶手段に記憶されている認証用素データに前記乱数を用いた乱数効果を施した後、認証用データとして第4の記憶手段に書き込み、証明データ検証手段は、第6の記憶手段に記憶されている乱数による乱数効果を、上記証明データ生成装置によって第5の記憶手段に書き込まれた証明データから除去した結果が、アクセス資格認証の特徴情報である復号鍵で第7の記憶手段に記憶されている認証用素データを復号したものであることを検証することを特徴とする請求項14に記載のアクセス資格認証機能付

きデータ記憶装置。

【請求項 17】 上記アクセス資格認証の特徴情報がデジタル署名関数の署名鍵であり、証明データ検証装置が乱数生成手段を備え、乱数生成手段は生成した乱数を認証用データとして第4の記憶手段に書き込み、証明データ検証手段は、証明データ生成装置によって第5の記憶手段に書き込まれた証明データが、前記乱数である認証用データに対する、アクセス資格認証の特徴情報である署名鍵によるデジタル署名であることを検証することを特徴とする請求項14に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 18】 暗号化関数が法 n のもとでの RSA 公開鍵暗号であり、アクセス資格認証の特徴情報が秘密鍵 D であり、秘密鍵 D に対応する公開鍵が E であり、証明データ検証手段は、第5の記憶手段に書き込まれた証明データ R を E 乗した結果と、第4の記憶手段に記憶されている認証用データ C とが、法 n のもとで合同であること ($R^E \bmod n = C \bmod n$) を検証することを特徴とする請求項15に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 19】 暗号化関数が法 n のもとでの RSA 公開鍵暗号であり、アクセス資格認証の特徴情報が秘密鍵 D であり、秘密鍵 D に対応する公開鍵が E であり、上記第7の記憶手段に記憶される認証用素データがデータ K を法 n のもとで E 乗した数 K' ($= K^E \bmod n$) であり、上記乱数生成手段は、生成した乱数 r を法 n のもとで E 乗した数と、前記 K' とを法 n のもとで乗じた数 C ($= r^E K' \bmod n$) を認証用データとして前記第4の記憶手段に書き込み、証明データ検証手段は、第6の記憶手段に記憶されている乱数 r の法 n のもとでの逆数を、証明データ生成装置によって第5の記憶手段に書き込まれた証明データ R に乗じた数と、前記 K とが法 n のもとで合同であること ($K \bmod n = r^{-1} R \bmod n$) を検証することを特徴とする請求項16に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 20】 暗号化関数が法 n のもとでの RSA 公開鍵暗号であり、アクセス資格認証の特徴情報が秘密鍵 D であり、秘密鍵 D に対応する公開鍵が E であり、上記第3の記憶手段に記憶される証明用補助情報 t が、前記 D から上記第2の記憶手段に記憶されるアプリケーションプログラムのユーザの固有情報 e を

減じ、さらに、前記 n と e に依存する非衝突性関数値 $\omega (=G(n, e))$ と n のオイラー数 $\phi(n)$ との積を加えて得られるデータ ($t = D - e + \omega \phi(n)$) であり、上記証明データ生成手段は、前記 t と、前記 e と、第 1 の記憶手段に書き込まれた認証用データ C とから、法 n のもとで C の D 乗 ($C^D \bmod n$) を計算することによって前記証明データを生成することを特徴とする請求項 18 または 19 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 21】 上記証明データ生成手段が、第 3 の演算手段と、第 4 の演算手段と、第 5 の演算手段とからなり、第 3 の演算手段は、前記法 n のもとで前記 C の前記 t 乗 ($C^t \bmod n$) を計算し、第 4 の演算手段は、前記法 n のもとで前記 C の前記 e 乗 ($C^e \bmod n$) を計算し、第 5 の演算手段は、前記法 n のもとで第 1 および第 2 の演算手段の計算結果を乗じることによって、証明データ $R (=C^t C^e \bmod n)$ を生成することを特徴とする請求項 20 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 22】 前記第 2 の記憶手段及び前記第 4 の演算手段が、内部の処理手段及びデータを外部の観測から防御する防御手段中に内蔵されることを特徴とする請求項 21 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 23】 暗号化関数が法 n のもとでの RSA 公開鍵暗号であり、アクセス資格認証の特徴情報が秘密鍵 D であり、秘密鍵 D に対応する公開鍵が E であり、上記第 3 の記憶手段に記憶される証明用補助情報 t が、前記 D に、上記第 2 の記憶手段に記憶されるアプリケーションプログラムのユーザの固有情報 e と前記法 n とに依存する非衝突性関数値 $F(n, e)$ を加えて得られるデータ ($t = D + F(n, e)$) であり、上記証明データ生成手段は、前記 t と、前記 e と、前記第 1 の記憶手段に書き込まれた認証用データ C とから、法 n のもとで C の D 乗 ($C^D \bmod n$) を計算することによって前記証明データを生成することを特徴とする請求項 18 または 19 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 24】 上記証明データ生成手段が、第 3 の演算手段と、第 4 の演算手段と、第 5 の演算手段とからなり、第 3 の演算手段は、前記法 n のもとで前記 C の前記 t 乗 ($C^t \bmod n$) を計算し、第 4 の演算手段は、前記法 n の

もとで前記Cの前記 $F(n, e)$ 乗($C^{F(n, e)} \bmod n$)を計算し、第5の演算手段は、前記法 n のもとで、第3の演算手段の計算結果と、第4の演算手段の計算結果の逆数とを乗じることによって、証明データ $R (= C^t C^{-F(n, e)} \bmod n)$ を生成することを特徴とする請求項23に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項25】 前記第2の記憶手段及び前記第4の演算手段が、内部の処理手段及びデータを外部の観測から防御する防御手段中に内蔵されることを特徴とする請求項24に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項26】 暗号化関数が法 p のもとでのPohlig-Hellman非対称鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵 D であり、鍵 D に対応する他方の鍵が E であり($DE \bmod p-1=1$)、証明データ検証手段は、第5の記憶手段に書き込まれた証明データ R を E 乗した結果と、第4の記憶手段に記憶されている認証用データ C とが法 p のもとで合同であること($R^E \bmod p = C \bmod p$)を検証することを特徴とする請求項15に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項27】 暗号化関数が法 p のもとでのPohlig-Hellman非対称鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵 D であり、鍵 D に対応する他方の鍵が E であり($DE \bmod p-1=1$)、上記第7の記憶手段に記憶される認証用素データがデータ K を法 p のもとで E 乗した数 K' ($= K^E \bmod p$)であり、上記乱数生成手段は、生成した乱数 r を法 p のもとで E 乗した数と、前記 K' とを法 p のもとで乗じた数 $C (= r^E K' \bmod p)$ を認証用データとして前記第4の記憶手段に書き込み、証明データ検証手段は、第6の記憶手段に記憶されている乱数 r の法 p のもとでの逆数を、証明データ生成装置によって第5の記憶手段に書き込まれた証明データ R に乗じた数と、前記 K とが法 p のもとで合同であること($K \bmod p = r^{-1} R \bmod p$)を検証することを特徴とする請求項16に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項28】 暗号化関数が法 p のもとでのPohlig-Hellman非対称鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵 D であり、鍵 D

に対応する他方の鍵が E であり ($DE \bmod p-1=1$)、上記第 3 の記憶手段に記憶される証明用補助情報 t が、前記 D に、上記第 2 の記憶手段に記憶されるアプリケーションプログラムのユーザの固有情報 e と前記 p とに依存する非衝突性関数値 $F(p, e)$ を加えて得られるデータ ($t=D+F(p, e)$) であり、上記証明データ生成手段は、前記 t と、前記 e と、第 1 の記憶手段に書き込まれた認証用データ C とから、法 p のもとで C の D 乗 ($C^D \bmod p$) を計算することによって前記証明データを生成することを特徴とする請求項 26 または 27 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 29】 上記証明データ生成手段が、第 3 の演算手段と、第 4 の演算手段と、第 5 の演算手段とからなり、第 3 の演算手段は、前記法 p のもとで前記 C の前記 t 乗 ($C^t \bmod p$) を計算し、第 4 の演算手段は、前記法 p のもとで、前記 $F(p, e)$ を指数として、前記 C のべき乗 ($C^{F(p,e)} \bmod p$) を計算し、第 5 の演算手段は、前記法 p のもとで、第 3 の演算手段の計算結果と、第 4 の演算手段の計算結果の逆数とを乗じることによって、証明データ R ($=C^t C^{-F(p,e)} \bmod p$) を生成することを特徴とする請求項 28 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 30】 前記第 2 の記憶手段及び前記第 4 の演算手段が、内部の計算手順及びデータを外部の観測から防御する防御手段中に内蔵されることを特徴とする請求項 29 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 31】 暗号化関数が法 p 、生成元 a のもとでの ElGamal 公開鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵 X であり、鍵 X に対応する公開鍵が Y であり ($Y=a^X \bmod p$)、 u が上記 a を法 p のもとで適当な乱数 z を指数としてべき乗した数であり ($u=a^z \bmod p$)、 K' が、上記 Y を法 p のもとで上記乱数 z を指数としてべき乗した数と、データ K との積であるとき ($K'=Y^z K \bmod p$)、上記第 7 の記憶手段に認証用素データとして u 及び K' の組が記憶され、上記乱数生成手段は、上記 u と、生成した乱数 r を前記 K' に法 p のもとで乗じた数 C ($=r K' \bmod p$) とを認証用データとして前記第 4 の記憶手段に書き込み、証明データ検証手段は、第 6 の記憶手段に記憶されている乱数 r の法 p のもとでの逆数を、証明データ生成装

置によって第5の記憶手段に書き込まれた証明データRに乗じた数と、前記Kとが法pのもとで合同であること ($K \bmod p = r^{-1} R \bmod p$) を検証することを特徴とする請求項16に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項32】 暗号化関数が法p、生成元aのもとでのElGamal公開鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵Xであり、鍵Xに対応する公開鍵がYであり ($Y = a^X \bmod p$)、上記第3の記憶手段に記憶される証明用補助情報tが、前記Xに、上記第2の記憶手段に記憶されるアプリケーションプログラムのユーザの固有情報eと前記pとに依存する非衝突性関数値 $F(p, e)$ を加えて得られるデータ ($t = X + F(p, e)$) であり、上記証明データ生成手段は、前記tと、前記eと、第1の記憶手段に書き込まれた認証用データu及びCから、法pのもとで、Cを上記uのX乗で割った数 ($C u^{-X} \bmod p$) を計算することによって上記証明データを生成することを特徴とする請求項31に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項33】 上記証明データ生成手段が、第3の演算手段と、第4の演算手段と、第5の演算手段とからなり、第3の演算手段は、前記法pのもとで前記uの前記t乗 ($u^t \bmod p$) を計算し、第4の演算手段は、前記法pのもとで前記uの前記 $F(p, e)$ 乗 ($u^{F(p, e)} \bmod p$) を計算し、第5の演算手段は、前記法pのもとで、上記Cを第3の演算手段の計算結果で割り、さらに、第4の演算手段の計算結果を乗じることによって、証明データR ($= C u^{-t} u^{F(p, e)} \bmod p$) を生成することを特徴とする請求項32に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項34】 前記第2の記憶手段及び前記第4の演算手段が、内部の計算手順及びデータを外部の観測から防御する防御手段中に内蔵されることを特徴とする請求項33に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項35】 署名関数が法p、生成元aのもとでのElGamal署名であり、アクセス資格認証の特徴情報が一方の鍵Xであり、鍵Xに対応する公開鍵がYであり ($Y = a^X \bmod p$)、証明データ検証手段は、第5の記憶手段に書き込まれた証明データR及びSに対して、法pのもとで、上記aを第4の

記憶手段に記憶されている認証用データCを指数としてべき乗した値と、上記YをR乗した値とRをS乗した値との積とが法pのもとで合同であること ($a^C \bmod p = Y^R R^S \bmod p$) を検証することを特徴とする請求項17に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項36】 署名関数が法p、生成元aのもとでのElGamal署名であり、アクセス資格認証の特徴情報が一方の鍵Xであり、鍵Xに対応する公開鍵がYであり ($Y = a^X \bmod p$)、上記第3の記憶手段に記憶される証明用補助情報tが、前記Xに、上記第2の記憶手段に記憶されるアプリケーションプログラムのユーザの固有情報eと前記pとに依存する非衝突性関数値F(p, e)を加えて得られるデータ ($t = X + F(p, e)$) であり、上記証明データ生成手段は、証明データR及びSを生成するに当たり、適当な乱数kを生成し、法pのもとでの上記aのk乗をR ($= a^k \bmod p$) とし、前記tと、前記eと、第1の記憶手段に書き込まれた認証用データCから、法p-1のもとで、CからXとrの積を引いた数にkの逆数を乗じることによって、S ($= (C - RX) k^{-1} \bmod p - 1$) を計算することを特徴とする請求項35に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項37】 第2の記憶手段及び証明データ生成手段が、内部の計算手順及びデータを外部の観測から防御する防御手段中に内蔵されることを特徴とする請求項36に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項38】 上記アプリケーションプログラムのユーザの固有情報が暗号関数の復号鍵であり、証明用補助情報がアクセス資格認証のための特徴情報を前記復号鍵に対応する暗号化鍵によって暗号化したものであり、第1の演算手段は上記アプリケーションプログラムのユーザの固有情報である復号鍵を用いて、証明用補助情報を復号することにより、アクセス資格認証のための特徴情報を算出することを特徴とする請求項4に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項39】 上記暗号関数が非対称鍵暗号関数であり、アプリケーションプログラムのユーザの固有情報が一方の鍵であることを特徴とする請求項38に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 40】 上記暗号関数が公開鍵暗号関数であり、アプリケーションプログラムのユーザの固有情報が秘密鍵であることを特徴とする請求項 39 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 41】 上記暗号関数が対称鍵暗号関数であり、アプリケーションプログラムのユーザの固有情報が共通秘密鍵であることを特徴とする請求項 38 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 42】 上記証明データ検証手段は、暗号化されたデータである上記認証用データあるいは上記認証用素データに対応する平文データを記憶する第 8 の記憶手段と、比較手段とを有し、上記比較手段は、上記証明データ生成手段が生成した上記証明データ或は証明データから乱数効果を除去した結果と、第 8 の記憶手段に記憶されている平文データを比較し、両者が一致した場合に限り、上記証明データが正当であると判断することを特徴とする請求項 8 または 16 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 43】 上記証明データ検証手段は、暗号化されたデータである上記認証用データあるいは上記認証用素データに対応する平文データに所定の一方方向関数を施した結果を記憶する第 9 の記憶手段と、上記一方方向関数を実行する第 6 の演算手段と、比較手段とを有し、第 6 の演算手段は、上記証明データ生成手段が生成した上記証明データに、必要ならば乱数効果を取り除いたのち、一方方向関数を施し、上記比較手段は、第 6 の演算手段による計算結果と、第 9 の記憶手段に記憶されているデータを比較し、両者が一致した場合に限り、上記証明データが正当であると判断することを特徴とする請求項 8 または 16 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 44】 上記証明データ検証手段は、プログラム実行手段を含み、上記認証用データあるいは上記認証用素データは、プログラムを暗号化して得られるデータであり、上記証明データ検証手段が、証明データ生成手段が生成した上記証明データを、必要ならば乱数効果を取り除いたのち、プログラムとしてプログラム実行手段に引き渡すことにより、証明データ生成手段が、暗号化されたプログラムである上記認証用データあるいは認証用素データを正しく復号した場合、即ち、暗号化されたプログラムが正しく復号された場合に限り、プログラム

実行手段が正しい動作を行うことを特徴とする請求項 8 または 16 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 45】 上記証明データ検証手段は、プログラム実行手段と、プログラム記憶手段と、プログラム復号手段とを含み、プログラム記憶手段に記憶されているプログラムは、その一部あるいは全部が暗号化されたものであり、上記認証用データあるいは上記認証用素データは、前記暗号化されたプログラムを復号するための復号鍵を別途暗号化して得られるデータであり、上記証明データ検証手段は、証明データ生成手段が生成した上記証明データをプログラム復号手段に引き渡し、プログラム復号手段は、前記証明データ生成手段が生成した証明データを、必要ならば乱数効果を取り除いたのち、復号鍵として用いることにより、プログラム記憶手段に記憶されたプログラムの必要な部分を復号し、プログラム実行手段が復号されたプログラムを実行することにより、証明データ生成手段が上記認証用データあるいは認証用素データを正しく復号した場合、即ち、暗号化されたプログラムを復号するために復号鍵が正しく復号された場合に限り、プログラム実行手段が正しい動作を行うことを特徴とする請求項 8 または 16 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 46】 上記証明データ生成装置および上記証明データ認証装置が同一の筐体内に設けられ、上記証明データ生成装置および上記証明データ認証装置が、当該筐体の外部の通信媒体を解さずに通信を行う請求項 14 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 47】 アプリケーションプログラムによる記憶媒体中のデータへのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記アプリケーションプログラムのユーザのアクセス資格を認証するアクセス資格認証機能付きデータ記憶装置において、

認証用データを記憶する第 1 の記憶手段と、

アプリケーションプログラムのユーザの固有情報を記憶する第 2 の記憶手段と

上記アプリケーションプログラムのユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶

する第 3 の記憶手段と、

上記第 1 の記憶手段に保持されている認証用データと、上記第 2 の記憶手段に記憶されている上記アプリケーションプログラムのユーザの固有情報とに所定の計算を施して証明データを生成する証明データ生成手段と、

記録媒体を備えこの記録媒体にデータを記憶保存するデータ記憶装置本体と、

上記アプリケーションプログラムに設けられ、上記データ記憶装置本体の記録媒体に記憶されたデータに対する操作を指示するコマンドを生成するコマンド生成手段と、

上記アプリケーションプログラムに設けられ、上記コマンド生成手段によって生成されたコマンドを上記アプリケーションプログラムの外部に発行するコマンド発行手段と、

上記証明データが上記アプリケーションプログラムのユーザの固有情報に基づいて生成されていることを検証する証明データ検証手段であって、上記証明データ生成手段によって生成された証明データと、上記第 3 の記憶手段に保持されている上記証明用補助情報とに所定の演算を施す演算手段を有し、上記演算手段の演算結果を使用して検証を行なう証明データ検証手段と、

上記データ記憶装置本体のデータに対する操作を指示するコマンドのうちの少なくとも 1 種類のコマンドについては、上記検証が成功した場合に限り上記コマンドの実行を許容するコマンド管理手段とを有することを特徴とするアクセス資格認証機能付きデータ記憶装置。

【請求項 4 8】 データ記憶装置の中の記憶媒体が、追記型の光記録媒体であることを特徴とする請求項 1 乃至 4 7 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 4 9】 データ記憶装置中の追記型の光記録媒体が、相変化方式光記録媒体であることを特徴とする請求項 4 8 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 5 0】 データ記憶装置中の追記型の光記録媒体が、相分離方式光記録媒体であることを特徴とする請求項 4 8 に記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 5 1】 データ記憶装置の記録媒体のうち少なくとも所定のアクセスログを最初に記憶する記憶媒体を追記型の光記憶媒体とすることを特徴とする請求項 1 乃至 5 0 記載のアクセス資格認証機能付きデータ記憶装置。

【請求項 5 2】 補助記憶手段として所定のアクセスログを最初に記憶する部分を追記型の光記憶媒体で構成することを特徴とするデータ記憶装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、データ記憶装置に関し、ネットワーク、特にインターネットと接続された情報空間におけるデータ記憶装置の安全性（セキュリティ）を向上させるようにしてものである。

【0 0 0 2】

【従来の技術】

〔関連技術〕

本発明に関連する従来技術として、ファイアウォール技術とファイル暗号化技術を挙げることができる。

【0 0 0 3】

ファイアウォール技術は、ファイアウォールゲートウェイと呼ばれるホストマシンを、内部ネットワークと外部ネットワークの接続点に配置し、外部ネットワークから内部ネットワークへの通信を監視し、安全な通信のみを内部ネットワークに接続する技術である。

【0 0 0 4】

一方、ファイル暗号化技術は、ハードディスクなどファイルを暗号化することでデータを保護する技術である。この技術は、外部ネットワークからの攻撃に限らず、内部ネットワークから行われる攻撃に対しても、機密データが読み出されることを防止する。また、記憶装置に記憶されるデータが破壊、改竄されることを防止する。

【0 0 0 5】

〔従来技術の問題点〕

最初に、ファイアウォール技術の問題点について述べる。

【0006】

いつでも、どこでも、誰でもという情報環境の理想を具現化するインターネットの普及は目覚しく、世界中の人間がインターネットに繋がるのもそう遠いことではないと予想されている。このインターネットにより形成された空間、サイバー空間（電脳空間）では、現在、現実世界の再構築が進行している。ビジネスもその例にもれず、一般にはサイバービジネスと呼ばれ新しいビジネス形態が次々と生まれつつある。このようにサイバー空間の利用が大きく進展しつつある反面、その問題点、課題も大きくクローズアップされてきている。問題／課題は大きく分けて2つあり、第1は、情報の自由な利用と、権利処理の両立であり、第2は情報の自由な利用と安全性の両立である。第1の問題は、著作権や知的財産権と情報の利用権の権利処理の問題である。この問題に対しては、元筑波大学教授の森亮一氏が超流通の考え方を提唱し（特公平6-95302号公報）、多くのメーカー、機関がこれに追随、実際に検討し、採用されつつある。第2の問題は、情報の安全性（機密性、真正性、保存性）に関する問題である。直接的には、第3者によるデータの破壊、盗聴、改竄に対する安全性の確保の問題である。

【0007】

インターネットを主体としたサイバー空間における情報の安全性（以下情報セキュリティと表現する）への脅威は、主に2つの攻撃（不正アクセス）に分類される。第1は、内なる敵と呼ばれるネットワーク内部の人間からの攻撃である。ここで、内部の人間とは、システム管理者や、システム構築者を含むネットワーク内のユーザーを指す。従来から、コンピュータ犯罪の多くは内部犯行といわれており、警察庁の統計によれば実に69%にものぼり、最近起こった事例からもそれは裏付けられている。第2は、第三者とよばれるネットワーク外からの侵入者であり、犯罪者、クラッカー、スパイ、産業スパイ、テロリスト等からなる。これは、インターネットがこれまでのある程度制限されたネットワークと異なり、不特定多数の人間に繋がっており、匿名性の高い情報システムだから起こり得るのである。インターネットが国境の無い無法地帯と例えられる所以はそこにある。第三者の脅威に対しては、トランザクション（transaction）に

おける盗聴を防止するための暗号技術や、ネットワーク内への侵入を防止するファイアウォールが主要な技術になっている。

【0008】

内部ネットワークには、様々なホストが接続されていて、それぞれが多様な処理を行っている。そして、必要とするセキュリティの用途やレベルも各ホストごとに異なる。しかしながら、ファイアウォール技術ではファイアウォールゲートウェイにおいて集中的にセキュリティを施すため、内部ネットワークに接続した各ホストの処理内容や通信のコンテキストに立脚した木目の細かいセキュリティを実現することは不可能であり、IPアドレスやポート番号といったプロトコルレベルの大雑把な情報のみを手掛かりに危険な通信を排除することとなる。このため、特定のホストにとって危険な通信が、ファイアウォールの監視の目を逃れて内部ネットワークに潜り込んでしまう可能性がある。

【0009】

また、ファイアウォールの利点のひとつは、全ての通信を特定のファイアウォールゲートウェイを経由させることで抜け漏れを排除する点にあるが、逆に見れば、ゲートウェイマシンが侵入されれば他に防御手段がないこととなってしまう。

【0010】

ファイル暗号化技術を用いることにより、ファイアウォールの上記の欠点を一部補うことが可能となる。即ち、個々のホストの利用形態に併せて、ファイルの暗号化及び鍵管理を行うことが可能となり、仮にファイアウォールゲートウェイが侵入された場合でも、ホストレベルでファイルの内容を保護することができる。

【0011】

しかしながら、ファイル暗号化技術が有効であるのは、ファイルの中身を読み出そうとする攻撃に対してであり、ファイルそのものを破壊することを目的とした攻撃に対処することはできない。実際、ファイルを破壊しようと試みる攻撃はファイルを読み出そうと試みる攻撃に比較して、はるかに容易に実行可能であり、攻撃が成功した場合の被害も同等に著しい。

【0012】

内なる敵、あるいは外部からの第三者のいずれにしろ、直接的な攻撃（アタック）はPC/WS（パーソナルコンピュータ/ワークステーション）の記録／蓄積部（メモリ／ストレージ部）上にある（保存されている）情報（ファイル）に対して行われる。攻撃の目的は情報の破壊、改竄、盗聴（漏洩）である。この内、盗聴対策は、情報の暗号化が主要な手段となっている。従って、盗聴は暗号を解読する必要があり、そう容易ではない。しかし、改竄、破壊は必ずしも暗号解読をする必要がなく、単に情報を書き換えたり消したりすれば良いので容易かつ、実害が大きい。また、記録／蓄積部への侵入者は必ずログ（ログ記録）を取られるが、ログを消すのがクラッカー、ハッカーの基本であり、侵入した証拠を消して退去する。

【0013】

そして、この侵入した証拠を消して退去するを可能にしている主な原因が、現行の記録／蓄積技術の中心である磁気記録媒体を用いるハードディスク装置（Hard Disk Drive）の書換え可能という特性に帰される。現実世界では、情報は紙に記録され、改竄や消去しようとする、何らかの証拠が残るので、それらの脅威に対して抑制力があつた。しかし、インターネットの時代になり、不特定多数の人間がネットワークに繋がり、しかも匿名性が高く、これらの不正行為をしても証拠を消せるため、破壊、改竄等の不正行為が誘発、助長される結果になっている。

【0014】

【発明が解決しようとする課題】

本発明は、以上の事情を考慮してなされたものであり、ホストレベルにおいて、記憶媒体に記憶されているファイルの読み出しのみならず、ファイルを破壊、改竄しようとする攻撃に対して有効な防御手段を提供することを目的としている。

【0015】

【課題を解決する手段】

本発明は上述の目的を達成するために特許請求の範囲の記載のとおり構成を

採用している。以下では、特許請求の範囲の記載内容について補充的な説明を行う。

【0016】

本発明の基本的な手段は次のようなものである。

【0017】

本発明の基本的な手段は2つの段階から成る。第1段階は、外部からの不正アクセスを防止するものであり、外部からのアクセスに対する認証手段により外部からの破壊、改竄、盗聴（漏洩）からなる攻撃を防止する。第2段階は上記第1段階の壁を通り抜けてきた不正アクセス、及び内なる敵からの不正アクセスによる改竄、破壊からなる攻撃を防止するものであり、改竄、破壊が物理的に不可能な記憶媒体により達成するものである。即ち、認証手段をアプリケーションの下レイヤー（層）に備え、認証手段を突破してくる者を防止する能力を既存の認証手段によるよりも強くすると同時に、その強化された認証手段をたとえ突破されてもさらに改竄・破壊に対する防御を完璧にする手段を提供しようとするものである。

【0018】

最初に、第1段階である外部からのアクセスに対する認証手段による攻撃防止方法について説明する。

【0019】

記憶媒体にアクセスしようとするアプリケーションプログラム（ホスト上で動作するプログラム）は、アクセス資格認証機能付きデータ記憶装置に対して、アクセスを要求するコマンドを送付する。アクセス資格認証機能付きデータ記憶装置は、アプリケーションプログラムがアプリケーションプログラムのユーザの固有情報と証明用補助データを用いて生成する証明データを検証し、検証に成功した場合に限りアクセスコマンドを受け付け、データ記憶装置にコマンドを発行する。

【0020】

このようにアクセス資格が認証された場合にのみデータ記憶装置へのデータアクセスが許されるようになっているので、データ記憶装置のデータを不正アクセ

スから確実に防護することができる。このスキームによるセキュリティは証明用補助情報によりアプリケーションプログラム（ユーザ）ごとに木目細かく設定できる。この構成では、ポート番号や要求元アドレス情報に基づく従来のファイアウォールによるセキュリティに対して極めて柔軟性に富むものである。もちろん、本発明のセキュリティスキームと従前のセキュリティスキームとを併用しても有効である。

【0021】

次に第2段階について説明する。第2段階は上記説明による第1段階の壁を通り抜けてきた不正アクセス、及び内なる敵からの不正アクセスによる破壊、改竄からなる攻撃を防止するものであり、破壊、改竄が物理的に不可能な記憶媒体により達成するものである。現状では、ほとんどのデータ記憶はハードディスク装置（以下HDD）に依っている。HDDは磁気記録媒体を用いた書換え可能なストレージであり、PC/WS（パーソナルコンピュータ/ワークステーション）のキャッシュメモリの下に有り、いわゆるワーキングメモリとして使用されることが多い。PC/WS上でユーザーがデータを作成/編集する上で、頻繁にデータの修正、変更をする場合、この書換え性は大切な要素である。しかし、重要な情報を記録して保存する場合には、その書き換え性は逆にセキュリティの面からの安全上、大きな問題、弱点になる。外部から侵入したシステム精通者や、例えば悪意のある内部システム管理者（システムアドミニストレータ）にとって、証拠を残さずに改竄・破壊をすることは非常に容易である。そのような犯行の場合、ログ記録さえも改竄されうるので犯行を見つけること自体が非常に困難を伴う事になる。さらに直接的な表現をすると、不正アクセス者の攻撃対象はまさにHDDという記憶/蓄積部なのである。

【0022】

一般に情報セキュリティの3要素として、機密性、真正性、可用性が挙げられる。これらの要件を記録/蓄積部（メモリ/ストレージ部）に対してブレークダウンすると、原本性、ネットワーク適性の2つになる。さらにこれらを具体的な要件にブレークダウンすると、原本性は、改竄不可能性と原本寿命に、ネットワーク適性は、転送レート、及び大容量性になる。改竄不可能とは、書換え不可能の

事である。原本寿命は、暗号寿命（暗号が陳腐化するのに要する時間）と同程度以上必要とされることから、20年以上が望ましいと考えられる。転送レートは、通常のHDDと同等以上が望ましい。ただし、必ずしも必要なものではなく、扱う情報の量、性質により適時設定される。大容量性は、これもHDDと同等以上のものが望ましい。

【0023】

世の中に知られている種々のストレージの中で、これらの要求に最も近いものは、追記型の光ストレージであることが分かる。

【0024】

追記型光ストレージは、改竄不可能性を除くと不満足な点もあるが、これらは将来改善されうる可能性があるのに対して、他のストレージでは改竄不可能を実現する事は現在と将来を含めて不可能である。この追記型の光ストレージは、具体的には、CD-R (Compact Disk Recordable)、DVD-R (Digital Versatile Disk Recordable)、及びISO (国際標準化機構)で規格化されたWO (Write-Once)型媒体である。容量は、採用されるシステムの必要とする容量を具備する必要がある。これは、必ずしも1枚当たりで満足させる必要はない。むしろ、ライブラリーとして、必要に応じて媒体を供給できるようにしておく方が、より柔軟性をもったシステムを構築できる。ただし、光ディスク自体は可換媒体であり、容易にライブラリー、及びドライブから物理的に取り外しができるために、その管理にはセキュリティという観点からなされなければならない。即ち、物理的にこの媒体にアプローチできる人間をあらかじめ限定しておき、それを何らかのハンドリングをする場合には、複数の人間による認証を必要とさせるような仕組みをつける必要がある。ライブラリーにおいては、媒体の格納庫とドライブ間のディスク媒体の受け渡し機構が当然ある。この受け渡しの時間、及び、ドライブに装着してから実際に稼動するまでの稼動時間、ヘッドのアクセスタイムが短ければ短いほど良い。ヘッドがアクセスした後は、実際のデータ転送レートがネットワークの速度についていけることが望ましい。その点では、HDD並の速度が要求される。現状では、約10Mbps程度の速度でしか記録できない。しかし、将来

、マルチビームヘッドにより飛躍的に転送速度が改善される可能性がある。次に原本寿命の点であるが、通常、追記型光ディスクの寿命は、10年以上が製品として保証されている。従って、一般には、さらに10年以上の寿命を確保する必要がある。追記型の光ディスク記録材料には、多くの種類があるが、原理上、分類すると、穴開け方式、相変態方式、合金化反応方式に分けられる。相変態方式には、結晶／非晶質間の相変化と、相の分離を利用した相分離法式がある。本発明において、上記要件を満たすものであれば何れ的方式でも用いることができる。

【0025】

本発明ではこのように追記型の記録媒体を用いることにより改竄等があってもこの証拠、痕跡がそのまま残るため、改竄等に対して有効に対処することが可能となる。

【0026】

さらに本発明を説明する。

【0027】

本発明の第1の側面によれば、上述の目的を達成するために、アプリケーションプログラムによる記憶媒体中のデータへのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記アプリケーションプログラムのユーザのアクセス資格を認証するアクセス資格認証機能付きデータ記憶装置に：認証用データを記憶する第1の記憶手段と；アプリケーションプログラムのユーザの固有情報を記憶する第2の記憶手段と；上記アプリケーションプログラムのユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第3の記憶手段と；上記第1の記憶手段に保持されている認証用データと、上記第2の記憶手段に記憶されている上記アプリケーションプログラムのユーザの固有情報と、上記第3の記憶手段に記憶されている上記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段と；記録媒体を備えこの記録媒体にデータを記憶保存するデータ記憶装置本体と；上記アプリケーションプログラムに設けられ、上記データ記憶装置本体の記録媒体に記憶されたデータに対する操作を指示するコマ

ンドを生成するコマンド生成手段と；上記アプリケーションプログラムに設けられ、上記コマンド生成手段によって生成されたコマンドを上記アプリケーションプログラムの外部に発行するコマンド発行手段と；上記証明データ生成手段によって生成された証明データが上記アクセス資格認証の特徴情報に基づいて生成されていることを検証する証明データ検証手段と；上記データ記憶装置本体のデータに対する操作を指示するコマンドのうちの少なくとも1種類のコマンドについては、上記検証が成功した場合に限り上記コマンドの実行を許容するコマンド管理手段とを設けるようにしている。

【0028】

この構成においてはアプリケーションプログラムごとに認証を行えるようにし、データ記憶装置のデータに対する不正のアクセスを回避できる。アプリケーションプログラムとデータ記憶装置とはネットワーク（LAN、WAN、インターネット）等で接続されたものでもよく、スタンドアローンの計算機にアプリケーションプログラムとデータ記憶装置とがともに存在するような構成であってもよい。

【0029】

また、上記データ記憶装置本体のデータに対する操作は、例えば、読み出し・書き換え・消去であり、少なくとも1種類のコマンドは書き換えまたは消去のコマンドである。

【0030】

本発明の第2の側面によれば、上述の目的を達成するために、アプリケーションプログラムによる記憶媒体中のデータへのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記アプリケーションプログラムのユーザのアクセス資格を認証するアクセス資格認証機能付きデータ記憶装置に：認証用データを記憶する第1の記憶手段と；アプリケーションプログラムのユーザの固有情報を記憶する第2の記憶手段と；上記アプリケーションプログラムのユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第3の記憶手段と；上記第1の記憶手段に保持されている認証用データと、上記第2の記憶手段に記憶されて

いる上記アプリケーションプログラムのユーザの固有情報とに所定の計算を施して証明データを生成する証明データ生成手段と；記録媒体を備えこの記録媒体にデータを記憶保存するデータ記憶装置本体と；上記アプリケーションプログラムに設けられ、上記データ記憶装置本体の記録媒体に記憶されたデータに対する操作を指示するコマンドを生成するコマンド生成手段と；上記アプリケーションプログラムに設けられ、上記コマンド生成手段によって生成されたコマンドを上記アプリケーションプログラムの外部に発行するコマンド発行手段と；上記証明データが上記アプリケーションプログラムのユーザの固有情報に基づいて生成されていることを検証する証明データ検証手段であって、上記証明データ生成手段によって生成された証明データと、上記第 3 の記憶手段に保持されている上記証明用補助情報とに所定の演算を施す演算手段を有し、上記演算手段の演算結果を使用して検証を行なう証明データ検証手段と；上記データ記憶装置本体のデータに対する操作を指示するコマンドのうちの少なくとも 1 種類のコマンドについては、上記検証が成功した場合に限り上記コマンドの実行を許容するコマンド管理手段とを設けるようにしている。

【 0 0 3 1 】

この構成においてもアプリケーションプログラムごとに認証を行えるようにし、データ記憶装置のデータに対する不正のアクセスを回避できる。なお、この構成では、アプリケーションプログラムがデータ記憶装置をアクセスするときに認証補助情報を送信して検証時に認証補助情報を用いた演算を行う必要がある。

【 0 0 3 2 】

また本発明の第 3 の側面によれば、上述の目的を達成するために、上述のようなデータ記録装置において、その記憶媒体を、追記型の光記録媒体としている。

【 0 0 3 3 】

この構成においては、データの改竄等があったときにも、それを知ることができる。データの改竄等に対して適切な対処を行うことができる。

【 0 0 3 4 】

この構成において、追記型の光記録媒体は、例えば相変化方式光記録媒体や、相分離方式光記録媒体である。

【0035】

また、データ記憶装置の記録媒体のうち少なくとも所定のアクセスログを記憶する記憶媒体が追記型の光記憶媒体とするようにしてもよい。すなわち、追記型の記録媒体と再書き込み可能な記録媒体とから記録装置を構成してもよい。この場合、所定のアクセスログを記憶する部分を追記型の光記憶媒体で構成するようにしてもよい。

【0036】

なお、上述ではアプリケーションのユーザのアクセス資格を認証してデータ記憶装置へのアクセスを制御するようにしたが、個々のアプリケーション自体のアクセス資格を認証してデータ記憶装置へのアクセスを制御する構成としてもよい。このアプリケーションとしては例えばJ A V A（米国サンマイクロシステムズ社商標）アプレットとしてサーバから取り出して実行するものでもよい。またアプリケーションサーバが提供するアプリケーションとしてもよい。このようにするとアプリケーションの管理を行ってセキュリティを実現できる。アプリケーションの利用におけるユーザ認証は、例えば、ディレクトリサーバを用いて認証を行なうことができる。

【0037】

この点をさらに説明する。すなわち、アプリケーションプログラムによる記憶媒体中のデータへのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記アプリケーションプログラムのアクセス資格を認証するアクセス資格認証機能付きデータ記憶装置に：認証用データを記憶する第1の記憶手段と；アプリケーションプログラムの固有情報を記憶する第2の記憶手段と；上記アプリケーションプログラムの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第3の記憶手段と；上記第1の記憶手段に保持されている認証用データと、上記第2の記憶手段に記憶されている上記アプリケーションプログラムの固有情報と、上記第3の記憶手段に記憶されている上記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段と；記録媒体を備えこの記録媒体にデータを記憶保存するデータ記憶装置本体と；上記アプリケーションプログラ

ムに設けられ、上記データ記憶装置本体の記録媒体に記憶されたデータに対する操作を指示するコマンドを生成するコマンド生成手段と；上記アプリケーションプログラムに設けられ、上記コマンド生成手段によって生成されたコマンドを上記アプリケーションプログラムの外部に発行するコマンド発行手段と；上記証明データ生成手段によって生成された証明データが上記アクセス資格認証の特徴情報に基づいて生成されていることを検証する証明データ検証手段と；上記データ記憶装置本体のデータに対する操作を指示するコマンドのうちの少なくとも1種類のコマンドについては、上記検証が成功した場合に限り上記コマンドの実行を許容するコマンド管理手段とを設ける。

【0038】

また、アプリケーションプログラムによる記憶媒体中のデータへのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記アプリケーションプログラムのアクセス資格を認証するアクセス資格認証機能付きデータ記憶装置に：認証用データを記憶する第1の記憶手段と；アプリケーションプログラムの固有情報を記憶する第2の記憶手段と；上記アプリケーションプログラムの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第3の記憶手段と；上記第1の記憶手段に保持されている認証用データと、上記第2の記憶手段に記憶されている上記アプリケーションプログラムの固有情報とに所定の計算を施して証明データを生成する証明データ生成手段と；記録媒体を備えこの記録媒体にデータを記憶保存するデータ記憶装置本体と；上記アプリケーションプログラムに設けられ、上記データ記憶装置本体の記録媒体に記憶されたデータに対する操作を指示するコマンドを生成するコマンド生成手段と；上記アプリケーションプログラムに設けられ、上記コマンド生成手段によって生成されたコマンドを上記アプリケーションプログラムの外部に発行するコマンド発行手段と；上記証明データが上記アプリケーションプログラムの固有情報に基づいて生成されていることを検証する証明データ検証手段であって、上記証明データ生成手段によって生成された証明データと、上記第3の記憶手段に保持されている上記証明用補助情報とに所定の演算を施す演算手段を有し、上記演算手段の演算結果を使用して検証を行なう

証明データ検証手段と；上記データ記憶装置本体のデータに対する操作を指示するコマンドのうちの少なくとも1種類のコマンドについては、上記検証が成功した場合に限り上記コマンドの実行を許容するコマンド管理手段とを設ける。

【0039】

なお、本発明は方法の発明としても実現することができ、また方法の発明の少なくとも一部をコンピュータプログラムとして実現することができる。さらにそのような方法の発明をコンピュータで実行させるために用いるコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体として実現することもできる。

【0040】

【発明の実施の形態】

まず、この発明の原理的な構成例について説明する。この構成例では、サーバクライアント構成のシステムを例にするが、単一の計算機システムにおいて同様な処理を行ってもよい。

【0041】

図1は、この構成例のサーバクライアントシステムを全体として示しており、この図において、サーバ1およびクライアント2がネットワーク3を介して接続されている。ネットワーク3はLAN、WAN、インターネットとすることができる。サーバ1はこの例ではデータベース管理システム(DBMS)サーバであり、コマンド管理装置4およびデータ記憶装置5を有している。サーバ1は例えばPC(パーソナルコンピュータ)サーバであり、補助記憶装置としてデータ記憶装置5を有している。データ記憶装置5は、慣用的に用いられるハードディスクドライブの変わりに用いられ、相変化方式光記憶媒体や相分離方式光記憶媒体を具備して追記型の記録が行えるものである。コマンド管理装置4は証明データ検証装置10を保持している。なお、サーバ1はワークステーションで構成してもよい。もちろん大型汎用機を用いたシステムとしてもよい。

【0042】

クライアント2は、例えばパーソナルコンピュータで構成されアプリケーション6が実行されるようになっている。アプリケーション6は証明データ生成装置

11、コマンド生成装置7、コマンド発行装置8を具備しており、サーバ1のデータ記憶装置5に対してデータの読み出し、書き換え、消去を行う。まずコマンド生成装置7が読み出し、書き換えまたは消去のコマンドを生成し、コマンド発行装置8がサーバ1のコマンド管理装置4にコマンドを発行する。また、証明データ生成装置11は証明データを生成し、この証明データがコマンドに併せてコマンド管理装置10へ送られる。

【0043】

なお、ここではコマンド発行装置7がデータ読み出し、書き換え、消去のコマンドを発行するようにしたが、コマンド発行装置7はサーバ1に対するジョブ（SQLジョブ）等コマンド生成の元となるジョブを発行してもよい。すなわち、クライアント1上のアプリケーションがサーバ1にジョブと証明データを送り、サーバ1がジョブからコマンドを生成するようにしてもよい。

【0044】

この構成では、クライアント2のアプリケーション6からコマンドおよび証明データがサーバ1に送られ、サーバ1のコマンド管理装置4がこれを受け取り、証明データ検証装置10が証明データに基づいてアプリケーション6のユーザのアクセス資格を検証し、検証が成功したら、コマンドに基づいてデータ記憶装置5をアクセス可能にする。

【0045】

なお、証明データ検証装置10はコマンド管理装置4と別に構成されていてもよい。

【0046】

図2はクライアント2の具体的な構成例を示しており、この図において、図2において、証明データ生成装置11、コマンド生成装置7およびコマンド発行装置8がアプリケーションのプログラムモジュールとして構成されている。また、ユーザの個人情報が、耐タンパー特性を有する証明用ハードウェア33（ICカード、ボードなど）に保持されている。証明データ生成装置11は破線で示すように証明用ハードウェア33に組み込むようにしてもよい。なお、図2において、32はオペレーティング・システム等の制御プログラムであり、34はハード

ウェア全般を示す。

【0047】

つぎに、サーバ1側の証明データ検証装置10およびクライアント側の証明データ生成装置11について図3を参照して説明する。

【0048】

図3において、サーバ1およびクライアント2の他の構成要素については説明の便宜上省略した。証明データ生成装置11はアクセスチケット生成装置12からアクセスチケット（証明用補助データ）13を受領するようになっている。証明データ検証装置10は検証ルーチン15を実行する。証明データ生成装置11はユーザ固有情報16およびアクセスチケット13を保持し、証明データ生成プログラム17を実行する。

【0049】

アクセスチケット生成装置12はデータ記憶装置5（図1）のセキュリティを管理する者や、信頼できる第三者に設けられている。アクセスチケット生成装置12はアクセス資格認証の特徴情報14およびユーザ固有情報16に基づいてアクセスチケット13を生成し、このアクセスチケット13が通信またはフロッピーディスク等送付を介してユーザに送られ、ユーザの証明データ生成装置11に保持される。この後、証明データ検証装置10は認証用データ18を証明データ生成装置11に送出する。証明データ生成装置11はアクセスチケット13およびユーザ固有情報16を用いて証明データ19を生成し、これを証明データ検証装置10に返信する。証明データ検証装置10は認証用データに基づいて証明データの正当性を検証する。すなわち、証明データが、認証用データとアクセス資格認証の特徴情報とに基づいて生成されたデータであることを検証する。

【0050】

証明データの正当性が検証されれば、ユーザのアクセス資格が認証され、これに応じて、データ記憶装置5へのアクセスが許される。

【0051】

ユーザによるアクセスチケットの取得に関しては、共通のセンターがユーザからの発行依頼に応じて生成して配布する方法と、アプリケーションプログラムの

作成者が、アクセスチケット発行プログラムやアクセスチケット生成装置の助けを借りて個別に生成する方法がある。

【0052】

生成されたアクセスチケットは、フロッピーディスク等の可搬型記憶媒体を介してユーザに配送されるものとしてもよいが、アクセスチケットが十分な安全性を備えていることから、電子メールなどを用いてネットワークを介して配送されるように構成してもよい。

【0053】

アクセスチケットの安全性とは、以下の二つの性質である。

【0054】

アクセスチケットは記名式であり、即ち、アクセスチケットが発行されたユーザ本人（正確には、アクセスチケット生成時に用いられたユーザ固有情報の保持者）だけが該アクセスチケットを用いて証明データ生成装置を正しく作動させることができる。従って、悪意の第三者がネットワークを盗聴し、他のユーザのアクセスチケットを不正に手に入れたとしても、この第三者がアクセスチケットの発行先である正規のユーザのユーザ固有情報を手に入れないかぎり、このアクセスチケットを利用することは不可能である。

【0055】

アクセスチケットはさらに厳密な安全性を保持している。即ち、悪意の第三者が任意個数のアクセスチケットを集めて、いかなる解析を行ったとしても、得られた情報をもとに別のアクセスチケットを偽造したり、証明データ生成装置の動作を模倣して認証を成立させるような装置を構成することは不可能である。

【0056】

【実施例】

つぎにより具体的な構成について実施例に即して説明する。

【0057】

〔第一の実施例〕

この発明における第一の実施例では、アクセスチケットは次の式1に基づいて生成されるデータである。

【0 0 5 8】

【数 1】

$$(1) \quad t = D - e + \omega \phi(n)$$

上式中の各記号は以下を表す。

【0 0 5 9】

n は RSA 法数、即ち、十分大きな二つの素数 p 、 q の積である ($n = p q$)

【0 0 6 0】

$\phi(n)$ は n のオイラー数、即ち、 $p-1$ と $q-1$ の積である ($\phi(n) = (p-1)(q-1)$)。

【0 0 6 1】

ユーザ固有情報 e は、ユーザ毎に異なる数であり、ユーザを識別するために用いられる。

【0 0 6 2】

アクセスチケット秘密鍵 D は、法数 n のもとでの RSA 秘密鍵であり、式 2 を満たす。

【0 0 6 3】

【数 2】

$$(2) \quad \gcd(D, \phi(n)) = 1$$

ここで、 $\gcd(x, y)$ は二数 x 、 y の最大公約数を表す。式 (2) によって表現される性質は、式 3 を満たす数 E が存在することを保証する。

【0 0 6 4】

【数 3】

$$(3) \quad ED \bmod \phi(n) = 1$$

E をアクセスチケット公開鍵と呼ぶ。

【0 0 6 5】

ω は、 n 及び e に依存して定まる数であり、 n あるいは e のいずれか一方が異なる場合、その値が容易に一致しない（衝突しない）ように定め る。 ω の定め方の一例として、一方向ハッシュ関数 h を利用して、式 4 のように ω を定める方

法もある。

【0066】

【数4】

$$(4) \quad \omega = h(n | e)$$

ただし、記号|はビット列の接合を表す。

【0067】

一方向ハッシュ関数とは、 $h(x) = h(y)$ を満たす相異なる x 、 y を算出することが著しく困難であるという性質をもつ関数である。一方向ハッシュ関数の例として、RSA Data Security Inc. によるMD2、MD4、MD5、米国連邦政府による規格SHS (Secure Hash Standard) が知られている。

【0068】

上記の説明中に現れた数において、 t 、 E 、 n は公開可能であり、残りの D 、 e 、 ω 、 p 、 q 、 $\phi(n)$ はチケットを作成する権利を有する者以外には秘密である必要がある。図を参照してさらに第一の実施例について詳細に説明する。図4は、この発明における第一の実施例の構成を示し、図5は図4におけるデータのフローを示している。図4において、証明データ検証装置10は、アクセスチケット公開鍵記憶部101、乱数発生部102、乱数記憶部103、受信データ記憶部105、検証部106、実行部107およびエラー処理部108を含んで構成されている。また、証明データ生成装置11は、受信データ記憶部111、第1演算部112、アクセスチケット記憶部113、第2演算部114、ユーザ固有情報記憶部115および証明データ生成部116を含んで構成されている。実行部107はデータアクセスのコマンドを実行するものである。

【0069】

つぎに動作について説明する。

【0070】

1. ユーザがアクセスすることによって、証明データ検証装置101が起動される。すなわち、アプリケーション6のコマンド発行生成装置7がデータアクセスのコマンドを生成すると、コマンド発行装置8がサーバのコマンド管理装置4に

コマンドを発行する。これに応じて証明データ検証装置が起動する。

【0071】

2. 証明データ検証装置10は、認証用データCとアクセスチケット公開鍵記憶部101に記憶されているRSA暗号の法数nとを、証明データ生成装置11中の受信データ記憶部111に書き込むが、この認証用データCは以下の方法で生成される。

【0072】

証明データ検証装置中の乱数発生部102によって、乱数rを、アクセスチケット公開鍵記憶部101に保持されているRSA法数nと互いに素になるように生成し、乱数記憶部103に記録する。更に、この乱数rを認証用データCとする。後述するように、この場合、証明データ生成装置11が返す証明データは、Cを法数nのもとのRSA暗号を用いて暗号化したものとなる。

【0073】

Cの値は乱数rそのものであることから、通信の度に異なる値となり、リプレイアタックを防止する効果をもつ。

【0074】

3. 証明データ生成装置11中の第1演算部112は、アクセスチケット記憶部113に記憶されているアクセスチケットtを取得し、受信データ記憶部111に書き込まれたRSA法数nのもとで、式5を実行し中間情報R'を得る。

【0075】

【数5】

$$(5) \quad R' = C^t \bmod n$$

【0076】

4. 証明データ生成装置11中の第2演算部114は、ユーザ固有情報記憶部115に記憶されているユーザの固有情報eを取得し、式6の計算を実行し差分情報Sを得る。

【0077】

【数6】

$$(6) \quad S = C^e \bmod n$$

【0078】

5. 証明データ生成装置 11 中の証明データ生成部 116 は、第 1 および第 2 演算部 112、114 から R' および S を得て、式 7 の計算を行ない R を得る。

【0079】

【数 7】

$$(7) \quad R = R' \cdot S \pmod{n}$$

【0080】

6. 証明データ生成装置 11 は R を証明データ検証装置 10 の受信データ記憶部 105 に返送する。

【0081】

7. 証明データ検証装置 10 中の検証部 106 は、まず、受信データ記憶部 105 に返された証明データ R と、アクセスチケット公開鍵記憶部 101 に保持されている公開指数 E および RSA 法数 n をもとに式 8 の計算を行なう。

【0082】

【数 8】

$$(8) \quad R^E \pmod{n}$$

次いで、この計算結果と、乱数記憶部 103 中に保持されている乱数 $C (= r)$ とを比較することにより、式 9 が成り立つことを確かめる。

【0083】

【数 9】

$$(9) \quad C \pmod{n} = R^E \pmod{n}$$

式 (9) が成立する場合は実行部 107 を起動してコマンド処理を実行し、成立しない場合はエラー処理部 108 を起動してエラー処理を行う。

【0084】

〔第二の実施例〕

この発明の第二の実施例における、アクセスチケット t の構成、証明データ証明装置の作用は、前記第一の実施例におけるそれと同一である。第一の実施例においては証明データは認証用データの暗号化であったのに対し、第二の実施例においては証明データ検証装置 10 が生成する認証用データは証明データの（乱数

効果付)暗号化であり、証明データ生成装置11は認証用データを復号して(乱数効果を維持したまま)証明データを生成する。図を参照してさらに第二の実施例について詳細に説明する。図6は、この発明における第二の実施例の構成を示し、図7は図6におけるデータのフローを示している。図6において、証明データ検証装置10は、アクセスチケット公開鍵記憶部101、乱数発生部102、乱数記憶部103、受信データ記憶部105、乱数化部121、認証用素データ記憶部122、乱数効果除去部123、および実行手段310を含んで構成されている。また、証明データ生成装置11は、受信データ記憶部111、第1演算部112、アクセスチケット記憶部113、第2演算部114、ユーザ固有情報記憶部115および証明データ生成部116を含んで構成されている。

【0085】

つぎに動作について説明する。

【0086】

1. ユーザがアクセスすることによって、証明データ検証装置10が起動される。クライアント2のコマンド発行装置8がコマンドをサーバ1のコマンド管理部に発行することにより証明データ検証装置10が起動されるようになっている点は、第一の実施例の場合と変わらない。

【0087】

2. 証明データ検証装置10は、認証用データCと、アクセスチケット公開鍵記憶部101に保持されているRSA暗号の法数nとの組を証明データ生成装置11中の受信データ記憶部111に書き込むが、認証用データCは以下の方法で生成される。

【0088】

証明データ検証装置中の乱数発生部102によって、乱数rをアクセスチケット公開鍵記憶部101に保持されているRSA法数nと互いに素になるように生成し、乱数記憶部103に記録する。乱数化部121は、アクセスチケット公開鍵記憶部101に格納されている公開指数Eと法数nを取得し、さらに認証用素データ記憶部122に記憶されているデータC'を取得して、式10の計算を行なう。

【0089】

【数10】

$$(10) \quad C = r^E C' \pmod{n}$$

ここで、認証用素データ C' はデータ K に対して関係式 11 を満たすように生成され、認証用素データ記憶部 122 に格納された値である。

【0090】

【数11】

$$(11) \quad C' = K^E \pmod{n}$$

ここで、データ K を証明データ検証装置に保持せず、代わりに、その暗号化の結果である C' のみを保持するように証明データ検証装置 10 を構成すれば、証明データ検証装置 10 からデータ K が漏洩する危険を回避することができる。

【0091】

基本的に見れば、認証用データ C は法数 n のもとで RSA 暗号を用いてデータ K を暗号化したものであり、証明データ生成装置 11 は C を法数 n のもとで RSA 暗号を用いて復号することによりデータ K を再現する。しかし、このままでは、証明データ検証装置 10 と証明データ生成装置 11 の間の通信は常に同一のものとなり、いわゆるリプレイアタックが可能となることから、乱数 r を用いて認証用データに乱数効果を与え、証明データ生成装置 11 が返すデータを検証する際に乱数効果を除去するように構成される。

【0092】

3. 証明データ生成装置 11 中の第1演算部 112 は、アクセスチケット記憶部 113 に記憶されているアクセスチケット t を取得し、受信データ記憶部 111 に書き込まれた RSA 法数 n のもとで式 12 を実行し中間情報 R' を得る。

【0093】

【数12】

$$(12) \quad R' = C^t \pmod{n}$$

【0094】

4. 証明データ生成装置 11 中の第2演算部 114 は、ユーザ固有情報記憶部 115 に記憶されているユーザの固有情報 e を取得し、式 13 の計算を実行し差分

情報 S を得る。

【0095】

【数 13】

$$(13) \quad S = C^e \bmod n$$

【0096】

5. 証明データ生成装置 11 中の証明データ生成部 116 は、第 1 および第 2 演算部 112、114 から R' および S を得て、式 14 の計算を行ない R を得る。

【0097】

【数 14】

$$(14) \quad R = R' S \bmod n$$

【0098】

6. 証明データ生成装置 11 は R を証明データ検証装置 10 の受信データ記憶部 105 に返送する。

【0099】

7. 証明データ検証装置 10 中の乱数効果除去部 123 は、乱数記憶部 103 中から先に生成した乱数 r と、受信データ記憶部 106 から証明データ R とを取り出し、式 15 の計算を行なう。

【0100】

【数 15】

$$(15) \quad K' = r^{-1} R \bmod n$$

証明データ生成装置 11 において用いられるアクセスチケット t とユーザの固有情報 e の組合せが正しい場合に限り、計算の結果得られた K' と K が一致することに注意せよ。

【0101】

計算された K' は、証明データ検証装置 10 中の実行手段 310 に引き渡されるが、実行手段 310 は K' = K が成立する場合に限りコマンド処理を実行する。

【0102】

以下に、証明データ検証装置 10 中の実行手段 310 の構成法を数例述べる。

【0103】

1. 図8の構成例

実行手段310中の記憶部310aに予めデータKを記憶しておく。実行部310中の比較部310bは、このKと証明データ生成装置11から送られた証明データRから乱数効果を除去して得られる K' とを直接比較し、 $K' = K$ が成立する場合に限りコマンド処理を実行し、成立しない場合には処理を中止するなどのエラー処理を実行する(図9)。

【0104】

この構成例には、検証に用いるデータKが装置中に現れるという安全上の弱点がある。例えば、証明データ検証装置10、特に、実行手段310が、ユーザのPCあるいはワークステーション上で動作するプログラムとして構成されている場合、プログラムを解析してKを窃取することは、困難であっても、必ずしも不可能ではない。Kの値がユーザの知るところとなり、更に、証明データ検証装置で生成される乱数が予想可能であると、証明データ生成装置の動作を模倣する装置を構成することが可能となり、なりすましによる不正アクセスが可能となる。

【0105】

2. 図10の構成例

上記の欠点を改善するため、記憶部310aに記憶されるデータをKそのものではなく、Kに前述の一方方向ハッシュ関数 h を施して得られるデータ $h(K)$ とすることもできる。一方方向ハッシュ関数の性質から、記憶部310aに記憶されるデータ y から、 $y = h(x)$ を満たす x を算出することは著しく困難である。

【0106】

実行部310は、入力データに対し一方方向ハッシュ関数を施した結果を返す変換部310cを有する。比較部310bは、上記変換部310cの出力 $h(K')$ と、記憶部310aに記憶されたデータ($= h(K)$)とを比較する(図11)。

【0107】

この方法例では、検証に用いるデータKがプログラム中に現れることがなく、また、記憶部310aに記憶された $h(K)$ からKを計算することが著しく困難

であることから、図 8 の例より安全であるといえる。

【0108】

この構成では、図 11 に示すようにコマンド処理を制御する。

【0109】

しかしながら、比較部 310b はプログラム中では条件文として構成され、証明データ検証装置 10、特に、実行手段 310 がユーザの PC あるいはワークステーション上で動作するプログラムであるような場合、即ち、プログラムの分析・改竄が比較的容易であるような構成では、該条件文をスキップするようにプログラムを改竄することが可能である点で、なお弱点を有している。

【0110】

3. 図 12 の構成例

第 3 の構成例では、証明データ検証装置 10 の実行部 310 (コマンド処理を実行するモジュール) のプログラムのコードの一部或は全部を暗号化したデータを認証用素データ C' として、認証用素データ記憶部 122 に保持する。即ち、K は実行部プログラムのコードの一部或は全部である。

【0111】

実行手段 310 は、証明データ生成装置 11 からの返信データから乱数効果を除去して得られるデータ K' を、プログラム中の予め定められた位置に埋め込む。すなわち実行手段 310 は、コードとしてのデータ K' を記憶するコード記憶部 310d とこのコードをプログラム中に取り込むコード取り込み部 310e と、プログラムを実行するコード実行部 310f とを有している。証明データ生成装置 11 が正しいデータを返信した場合、即ち、K' = K である場合に限りプログラムは実行可能となる (図 13)。

【0112】

この構成例では、データアクセス用のプログラムの実行に不可欠なコードの一部或は全部が暗号化されているため、実行手段 310 がユーザの PC あるいはワークステーション上で動作するプログラムとして構成されているような比較的安全性の低い場合でも、不正実行を防止することができる。

【0113】

実行手段 310 がユーザの PC あるいはワークステーション上で動作するプログラムとして構成されている場合を例にとって、更に詳細な構成を述べる。

【0114】

証明データが書き込まれるコード記憶部 310d は、計算機中の指定された記憶領域である。

【0115】

コード実行部 310f は計算機の CPU 及び OS である。CPU と OS とは協力して、計算機のプログラム領域に記憶されている実行命令を順に実行する。特定の機能を提供する一連の実行命令をプログラムコードと呼ぶ。

【0116】

コード取込み部 310e の実体は、実行手段 310 中で最初に実行されるプログラムコードである。コード取込み部 310e は、直接・間接にコード記憶部 310d のアドレスをコード実行部 310f に指示することが可能である。例えば、コード取込み部 310e はコード記憶部 310d の物理アドレスを直接コード実行部 310f に指示してもよいし、計算機の OS が仮想アドレッシングを実行する場合には、コード取込み部 310e はコード記憶部 310d の仮想アドレスを指示し、OS が CPU 経由で受け取った仮想アドレスを物理アドレスに変換する方法でもよい。

【0117】

コード記憶部 310d に証明データが書き込まれた状態で、プログラムであるコード取込み部 310e が起動されると、コード取込み部 310e は、コード記憶部 310d のアドレスに記憶されている内容を計算機上のプログラム領域の特定のアドレスに書き出すよう、コード実行部 310f に命令し、実行させる。

【0118】

次いで、コード取込み部 310e は、コード実行部 310f に命令してコード記憶部 310d の記憶内容を書き出させた、プログラム領域中の特定のアドレスの実行命令を実行するよう、JMP 命令等を用いてコード実行部 310f に命令する。

【0119】

この構成例では、証明データが証明データ生成装置 11 によって正しく生成されたならば、乱数効果を取り除いた後のデータはプログラムコード、即ち、コード実行部 310f への一連の実行命令である。従って、上記構成では、コード取込み部 310e のプログラムコードに引続き、証明データ生成手段 11 によって復号されたプログラムコードが実行されることとなる。

【0120】

4. 図 14 の構成例

第 3 の構成例において、暗号化したコードを復号するために必要な復号鍵を、K とすることもできる。この構成によると、暗号化するコードのサイズに関わらず、K のサイズ、すなわち認証用素データ C' のサイズを一定の小さい値に抑えることが可能となり、通信のオーバーヘッドを減少させることができる。

【0121】

実行部 310 は、証明データ生成装置 11 からの返信データから乱数効果を除去して得られるデータ K' を用いて、プログラム中の予め定められた領域のコードを復号する。すなわち実行部 310 は暗号化されたプログラムを記憶するプログラム記憶部 310g と、暗号化されたプログラムを読み出しデータ K' を利用して復号する復号部 310h と、復号されたコードを取り出すコード取り出し部 310i と、取り出されたコードを実行するコード実行部 310f とを有する。

【0122】

実行手段 310 がユーザの PC あるいはワークステーション上で動作するプログラムとして構成されている場合を例にとって、更に詳細な構成を述べる。

【0123】

暗号化されたプログラムコードが記憶されているプログラム記憶部 310g は、計算機中の指定された記憶領域である。

【0124】

コード実行部 310f は計算機の CPU 及び OS である。

【0125】

プログラム記憶部 310g は、ハードディスク等、補助記憶装置上のファイル領域であるとしてもできる。即ち、暗号化されたプログラムコードは、ファ

イルとして記憶されている。

【0126】

復号部 310h の実体は、実行手段 310 中で最初に実行されるプログラムコードである。復号部 310h は、直接・間接に、プログラム記憶部 310g のアドレスを、コード実行部 310f に指示することが可能である。

【0127】

K' が与えられた状態で、プログラムである復号部 310h が起動されると、復号部 310h は、プログラム記憶部 310g に記憶されているデータを順に、あるいは定められた長さのブロック毎に読み出し、そのデータに K' を復号鍵とした所定の復号処理を実行し、その復号結果を計算機上のプログラム領域の特定のアドレスに書き出すよう、コード取り出し部 310i に命令し、実行させる。この処理により、プログラム記憶部 310g に記憶されていた暗号化データに対し、K' を復号鍵として、所定の復号アルゴリズムを実行した結果を、プログラム領域中の特定の位置に書き込んだこととなる。

【0128】

次いで、復号部 310h は、コード実行部 310f に命令して復号したプログラムコードを書き出させた、プログラム領域中の特定のアドレスの実行命令を実行するよう、JMP 命令等を用いてコード実行部 310f に命令する。

【0129】

この構成例では、証明データが証明データ生成装置 11 によって正しく生成されたならば、乱数効果を取り除いたのちの値はプログラム記憶部 310g に記憶されている暗号化されたプログラムコードを正しく復号するための復号鍵となる。復号部 310h は、この復号鍵を用いて、前記暗号化プログラムコードを復号し、復号結果であるプログラムコードをプログラム領域にロードし、ロードされた前記プログラムコードを実行するようコード実行部 310f に命令する。従って、上記構成では、復号部 310h のプログラムコードに引続き、証明データ生成手段 11 によって復号された復号鍵を用いて復号されたプログラムコードが実行されることとなる（図 15）。

【0130】

【第三の実施例】

この発明における第三の実施例では、アクセスチケット t は次の式 16 に基づいて生成されるデータである。

【0131】

【数 16】

$$(16) \quad t = D + F(n, e)$$

上式中の各記号は以下を表す。

【0132】

n は RSA 法数、即ち、十分大きな二つの素数 p 、 q の積である ($n = p q$)

【0133】

ユーザ固有情報 e はユーザ毎に異なる数であり、ユーザを識別するために用いられる。

【0134】

$\phi(n)$ は n のオイラー数、即ち、 $p-1$ と $q-1$ の積である ($\phi(n) = (p-1)(q-1)$)。

【0135】

アクセスチケット秘密鍵 D は、法数 n のもとでの RSA 秘密鍵であり、式 17 を満たす。

【0136】

【数 17】

$$(17) \quad \gcd(D, \phi(n)) = 1$$

ここで、 $\gcd(x, y)$ は二数 x 、 y の最大公約数を表す。式 (17) によって表現される性質は、式 18 を満たす数 E が存在することを保証する。

【0137】

【数 18】

$$(18) \quad ED \bmod \phi(n) = 1$$

E をアクセスチケット公開鍵と呼ぶ。

【0138】

二変数関数 $F(x, y)$ は関数値が衝突しにくい二変数関数であり、例えば、前述の一方方向ハッシュ関数 h を利用して、式 19 のように定めることができる。

【0139】

【数 19】

$$(19) \quad F(x, y) = h(x \parallel y)$$

図を参照してさらに第二の実施例について詳細に説明する。図 16 は、この発明における第三の実施例の構成を示し、図 17 は図 16 におけるデータのフローを示している。図 16 において、証明データ生成装置 11 は、受信データ記憶部 111、第 1 演算部 112、アクセスチケット記憶部 113、第 2 演算部 114、ユーザ固有情報記憶部 115、証明データ生成部 116 および指数生成部 130 を含んで構成されている。証明データ検証装置 10 は第一の実施例（図 4）や第二の実施例（図 6）の構成を採用することができる。ここでは説明を繰り返さない。

【0140】

つぎにこの構成における動作について説明する。

【0141】

1. ユーザがアクセスすることによって、証明データ検証装置 10 が起動される。すなわち、アプリケーション 6 のコマンド発行生成装置 7 がデータアクセスのコマンドを生成すると、コマンド発行装置 8 がサーバのコマンド管理装置 4 にコマンドを発行する。これに応じて証明データ検証装置が起動する。

【0142】

2. 証明データ検証装置 10 は、認証用データ C とアクセスチケット公開鍵記憶部 101 に記憶されている RSA 暗号の法数 n との組を証明データ生成装置 11 中の受信データ記憶部 111 に書き込む。

【0143】

C の生成方法としては、第一の実施例で述べた方法、第二の実施例で述べた方法のいずれも適用可能であるので、ここでは特に限定しない。前記いずれかの方法で生成された C が証明データ生成装置 11 中の受信データ記憶部 111 に書き込まれるものとする。

【0144】

3. 証明データ生成装置 11 中の第 1 演算部 112 は、アクセスチケット記憶部 113 に記憶されているアクセスチケット t を取得し、受信データ記憶部 111 に書き込まれた RSA 法数 n のもとで式 20 を実行し中間情報 R' を得る。

【0145】

【数 20】

$$(20) \quad R' = C^t \bmod n$$

【0146】

4. 証明データ生成装置 11 中の指数生成部 130 は、ユーザ固有情報記憶部 115 に記憶されているユーザの固有情報 e を取得し、式 21 の計算を実行する。

【0147】

【数 21】

$$(21) \quad F(n, e)$$

【0148】

5. 証明データ生成装置 11 中の第 2 演算部 114 は、指数生成部 130 で生成されたデータを用いて、式 22 の計算を実行し差分情報 S を得る。

【0149】

【数 22】

$$(22) \quad S = C^{F(n,e)} \bmod n$$

【0150】

6. 証明データ生成装置 11 中の証明データ生成部 116 は、第 1 および第 2 演算部 112、114 から R' および S を得て、式 23 の計算を行ない R を得る。

【0151】

【数 23】

$$(23) \quad R = R' \cdot S^{-1} \bmod n$$

ただし、 S^{-1} は法 n のもとでの S の逆数、即ち、式 24 を満たす数を表す。

【0152】

【数 24】

$$(24) \quad S \cdot S^{-1} \bmod n = 1$$

【0 1 5 3】

7. 証明データ生成装置 1 1 は R を証明データ検証装置 1 0 の受信データ記憶部 1 0 5 に返送する。

【0 1 5 4】

8. 証明データ検証装置 1 0 では、証明データ生成装置 1 1 から受け取った証明データの検証を行うが、その検証方法は、認証用データの一部である C の生成方法によって異なる。

【0 1 5 5】

C が第一の実施例の方法に基づいて生成されたものであれば、その検証は第一の実施例に述べられた方法に従って行われる。

【0 1 5 6】

C が第二の実施例の方法に基づいて生成されたものであれば、その検証は第二の実施例に述べられた方法に従って行われる。

【0 1 5 7】

[第四の実施例]

第四の実施例では、第一乃至第三の実施例において、証明データ生成装置がユーザの PC あるいはワークステーション上のプログラムと、前記 PC あるいはワークステーションに装着される IC カード、あるいは PC カード (PCMCIA カード) などの携帯可能な演算手段によって構成される場合について述べる。

【0 1 5 8】

第一乃至第三の実施例の証明データ生成装置 1 1 において、ユーザ固有情報 e は秘密情報であり、外部に漏洩しないよう注意を払わなければならない。また、ユーザ固有情報 e を用いた計算を実行する第 2 演算部 1 1 4 の動作が観測されるとユーザ固有情報 e が漏洩する危険がある。第三の実施例における関数 $F(x, y)$ の計算過程が観測された場合も同様である。即ち、ユーザ固有情報 e の漏洩を防ぐためには、ユーザ固有情報記憶部 1 1 5、第 2 演算部 1 1 4 及び指数生成部 1 3 0 の内部が外部から観測されることを防止しなければならない。この目的を達成するためには、証明データ生成装置 1 1 の一部をハードウェアとして構成すると有効である。

【0159】

このようなハードウェアとして、ICカード・PCカードのような携帯性のある手段を用いることにすれば、更にユーザの利便性を高めることができる。証明データ生成装置の内、ユーザに固有な部分は、ユーザ固有情報記憶部とアクセスチケット記憶部のみである。従って、例えば、ユーザ固有情報記憶部115と、アクセスチケット記憶部113と、第2演算部114と、指数生成部130とをICカード・PCカード中に構成し、証明データ生成装置の残りの部分をユーザが使用するPCあるいはワークステーション上で動作するプログラムとして構成することにすれば、証明データ生成装置11のうち各ユーザに固有な部分は、それぞれのユーザが携帯可能なICカード・PCカードとして実現され、ユーザに依存しない共通部分はプログラムとして任意のPCあるいはワークステーションに共通に構成されることとなる。このような構成によって、どのユーザでも、自分のICカード・PCカードを、前記プログラムがインストールされた任意のPCあるいはワークステーションに装着するだけで、該PCあるいはワークステーションを自分用の証明データ生成装置として利用することが可能となる。

【0160】

さて、内部メモリーに格納されたデータやプログラムが外部から観測されたり、改竄されたりすることを防止するための特殊な構成を持つハードウェアを、耐タンパーハードウェア（タンパーレジスタントハードウェア）と呼ぶ。耐タンパーハードウェアの構成法としては、例えば、特許第1863953号、特許第1860463号、特開平3-100753号公報等が知られている。

【0161】

特許第1863953号においては、情報記憶媒体の周囲に、各種の導体パターンを持つ複数のカードからなる包囲体を設ける。検出される導体パターンが予測されるパターンと異なる時に記憶情報を破壊する。

【0162】

特許第1860463号においては、情報記憶媒体の周囲に導体巻線を形成するとともに積分回路等からなる検知回路を設けることで、電子回路領域への侵入があった場合には電磁エネルギーの変動を検知し記憶情報を破壊する。

【0163】

特開平3-100753号公報においては、ハードウェア内部に光検知器を設け、ハードウェアに力が加えられて破壊された場合や穿孔されたときに入る外光を光検知器が検知し、記憶破壊装置が記憶情報をリセットする。

【0164】

これらの耐タンパーハードウェアを、ICカードやPCカード（PCMCIAカード）のような携帯可能な演算装置として実現することにより、ユーザに対する更なる利便を提供することができる。

【0165】

また、ICカードに実装されるマイクロコントローラーは、高密度実装ゆえに、それ自体で相当の耐タンパー特性を有しているとされている。

【0166】

図18は、第一および第二の実施例において、ユーザ固有情報eを保持するユーザ固有情報記憶手段115と、差分情報を生成する第二演算手段114とが、ICカードのような耐タンパーハードウェア160に封入されている構成を示している。

【0167】

図19は、第三の実施例において、ユーザ固有情報eを保持するユーザ固有情報記憶部115と、差分情報を生成する第2演算部114に加えて、指数生成部130も耐タンパーハードウェア161に封入されている構成を示している。

【0168】

ICカード側I/F部141は、ホストとICカードの通信を司るICカード側インターフェースであり、具体的には、通信用バッファと通信プログラムから構成される。証明データ生成装置の内の残りの部分は、ユーザのPCあるいはワークステーション上で動作するプログラムとして構成される。耐タンパーハードウェア160あるいは161中の各手段の作用は第一乃至第三の実施例に述べた通りであるので、以下では、その部分の作用については解説しない。また、説明を簡略にする目的で耐タンパーハードウェアをICカードであるものと仮定するが、この仮定はこの発明の一般性をなんら束縛するものではない。図20は、図

18におけるデータのフローを示している。

【0169】

つぎに、動作について説明する。

【0170】

1. ユーザがアクセスすることによって、証明データ検証装置10が起動される。

【0171】

2. 証明データ検証装置10は、認証用データCとアクセスチケット公開鍵記憶部101に記憶されているRSA暗号の法数nとの組を証明データ生成装置11中の受信データ記憶部111に書き込む。

【0172】

3. 証明データ生成装置11中のホスト側インターフェース部140は、受信データ記憶部111に書き込まれた認証用データCとnを、ICカード側インターフェース部141に引き渡す。ホスト側インターフェース部140は、ICカード中に設けられたICカード側インターフェース部141と協調して、ホスト・ICカード間のデータ通信を司る。

【0173】

4. アクセスチケット検索部142は、RSA法数nを検索のキーとして、アクセスチケット記憶部113に記憶されているアクセスチケットtを検索・取得する。

【0174】

5. 第1演算部112は、受信データ記憶部111に書き込まれたRSA法数nのもとで式25を実行し中間情報R'を得る。

【0175】

【数25】

$$(25) \quad R' = C^t \bmod n$$

【0176】

6. 次いで、ホスト側インターフェース部140は、ICカード側インターフェース部141にコマンドを発行し、その返り値として差分情報Sを得る。

【0177】

アクセスチケット及びICカード中の手段が第一あるいは第二の実施例に即して構成されている場合には、差分情報Sは式26によって計算される値である。

【0178】

【数26】

$$(26) \quad S = C^e \bmod n$$

【0179】

7. 証明データ生成装置11中の証明データ生成部116は、第1および第2演算部112、114からR' およびSを得て、式27の計算を行ないRを得る。

【0180】

【数27】

$$(27) \quad R = R' \cdot S \bmod n$$

【0181】

8. 証明データ生成装置11はRを証明データ検証装置10の受信データ記憶部105に返送する。

【0182】

上記の作用において、中間情報R' と差分情報Sの計算が、ユーザのPCあるいはワークステーションであるホスト側と、演算機能を内蔵するICカード側で並列に実行されるため、証明データ生成手段11が認証用データC及び法数nを受け取ってから、証明データRを計算するまでの実行時間を短縮することができ、よって処理効率を向上させている。

【0183】

この実施例では、アクセスチケット記憶部113には複数のアクセスチケットが記憶されるが、アクセスチケットが異なればそのRSA法数nが異なるので、アクセスチケットは、nをキーとして検索ができるようにnと対応づけて記憶される。

【0184】

また、アプリケーションやサーバがアクセス制御のために利用するRSA法数nは、アプリケーションやサーバ毎に異なるのが基本である。

【0 1 8 5】

アクセスチケット検索部 1 4 2 は、証明データ検証装置 1 0 から与えられる R S A 法数 n をキーとして、適切なアクセスチケットを検索し、以後の証明データの生成に供する。この検索機能により、証明データ生成装置 1 1 は、ユーザになんら負担を強いることなく、アクセスしている対象（個別のアプリケーションや個別のサーバ）に応じて適切な証明データを計算し、返送することが可能となる。

【0 1 8 6】

〔第五の実施例〕

この発明における第五の実施例では、第三の実施例で用いた R S A 公開鍵暗号の代わりに、P o h l i g - H e l l m a n 非対称鍵暗号を用いる。

【0 1 8 7】

P o h l i g - H e l l m a n 非対称鍵暗号は、法数として大きな素数 p を用いる点で、法数として 2 つの素数の積 $n (= p q)$ を用いる R S A 公開鍵暗号と異なる外は、R S A 公開鍵暗号と同一の暗号方式である。しかし、R S A 公開鍵暗号では、一方の鍵 E と法数 n から、もう一方の鍵 D を計算することが非常に困難であったため、 E 及び n を公開鍵として用い、 D を個人の秘密として用いることが可能であった。一方、P o h l i g - H e l l m a n 非対称鍵暗号暗号では、 E と p とから、容易に D が計算できるため、 E と p とを公開鍵として用いることはできない。即ち、 E と D との両方を当事者間の秘密としておく必要があり、DES (Data Encryption Standard) のような共通鍵暗号と同様の利用形態を採らざるを得ない。

【0 1 8 8】

この実施例では、アクセスチケット t は次の式 2 8 に基づいて生成されるデータである。

【0 1 8 9】

〔数 2 8〕

$$(28) \quad t = D + F(p, e)$$

上式中の各記号は以下を表す。

【0190】

p は十分大きな素数である。

【0191】

ユーザ固有情報 e はユーザ毎に異なる数であり、ユーザを識別するために用いられる。

【0192】

アクセスチケット秘密鍵 D は、法数 p のもとでの P o h l i g - H e l l m a n 暗号の鍵の一方であり、式 29 を満たす。

【0193】

【数 29】

$$(29) \quad \text{gcd}(D, p-1) = 1$$

ここで、 $\text{gcd}(x, y)$ は二数 x、y の最大公約数を表す。

【0194】

式 29 によって表現される性質は、式 30 を満たす数 E が存在することを保証する。

【0195】

【数 30】

$$(30) \quad ED \bmod p-1 = 1$$

二変数関数 $F(x, y)$ は関数値が衝突しにくい二変数関数であり、例えば、前述の一方ハッシュ関数 h を利用して、式 31 のように定めることができる。

【0196】

【数 31】

$$(31) \quad F(x, y) = h(x \parallel y)$$

つぎに、図 21 および図 22 を参照して第五の実施例についてさらに詳細に説明する。図 21 は第五の実施例の構成を示し、図 22 は図 21 におけるデータのフローを示している。図 21 において、証明データ検証装置 40 は、鍵記憶部 401、乱数発生部 402、乱数記憶部 403、受信データ記憶部 405、乱数化部 421、認証用素データ記憶部 422、乱数効果除去部 423 および実行手段 310 を含んで構成されている。また、証明データ生成部 41 は、受信データ記

憶部 411、第1演算部 412、アクセスチケット記憶部 413、第2演算部 414、ユーザ固有情報記憶部 415、証明データ生成部 416、および指数生成部 430を含んで構成されている。

【0197】

つぎに、動作について説明する。

【0198】

1. ユーザがアクセスすることによって、証明データ検証装置 40 が起動される。

【0199】

2. 証明データ検証装置 40 は、認証用データ C と鍵記憶部 401 に記憶されている法数 p との組を証明データ生成装置 41 中の受信データ記憶部 411 に書き込む。

【0200】

この実施例では、C の生成方法としては、第二の実施例で述べた方法に準じた方法によるものとするが、第一の実施例で述べた方法に準じた方法を構成することも難しくない。

【0201】

証明データ検証装置中 40 の乱数発生部 402 によって、乱数 r を鍵記憶部 401 に保持されている法数 p と互いに素になるように生成し、乱数記憶部 403 に記録する。乱数化部 421 は、鍵記憶部 401 に格納されている指数 E と法数 p を取得し、さらに認証用素データ記憶部 422 に記憶されている データ C' を取得して、式 32 の計算を行なう。

【0202】

【数 32】

$$(32) \quad C = r^E C' \mod p$$

ここで、認証用素データ C' はデータ K に対して関係式 33 を満たすように生成され、認証用素データ記憶部 305 に格納された値である。

【0203】

【数 33】

$$(33) \quad C' = K^E \bmod p$$

【0204】

3. 証明データ生成装置 4 1 中の第 1 演算部 4 1 2 は、アクセスチケット記憶部 4 1 3 に記憶されているアクセスチケット t を取得し、受信データ記憶部 4 1 1 に書き込まれた RSA 法数 p のもとで式 3 4 を実行し中間情報 R' を得る。

【0205】

【数 3 4】

$$(34) \quad R' = C^t \bmod p$$

【0206】

4. 証明データ生成装置 4 1 中の指数生成部 4 3 0 は、ユーザ固有情報記憶部 4 1 5 に記憶されているユーザの固有情報 e を取得し、式 3 5 の計算を実行する。

【0207】

【数 3 5】

$$(35) \quad F(p, e)$$

【0208】

5. 証明データ生成装置 1 1 中の第 2 演算部 4 1 4 は、指数生成部 4 3 0 で生成されたデータを用いて、式 3 6 の計算を実行し差分情報 S を得る。

【0209】

【数 3 6】

$$(36) \quad S = C^{F(p,e)} \bmod p$$

【0210】

6. 証明データ生成装置 4 1 中の証明データ生成部 4 1 6 は、第 1 および第 2 演算部 4 1 2、4 1 4 から R' および S を得て、式 3 7 の計算を行ない R を得る。

【0211】

【数 3 7】

$$(37) \quad R = R' S^{-1} \bmod p$$

ただし、 S^{-1} は法 p のもとでの S の逆数、即ち、式 3 8 を満たす数を表す。

【0212】

【数 3 8】

$$(38) \quad SS^{-1} \bmod p = 1$$

【0213】

7. 証明データ生成装置 41 は R を証明データ検証装置 40 の受信データ記憶部 405 に返送する。

【0214】

8. 証明データ検証装置 10 中の乱数効果除去部 423 は、乱数記憶部 403 中から先に生成した乱数 r を取り出し、式 39 の計算を行なう。

【0215】

【数 39】

$$(39) \quad K' = r^{-1}R \bmod p$$

証明データ生成装置 41 において用いられるアクセスチケット t とユーザの第一の固有情報 e の組合せが正しい場合に限り、計算の結果得られた K' と K が一致することに注意せよ。

【0216】

【第六の実施例】

この発明の第六の実施例では、第三の実施例における RSA 公開鍵暗号の代わりに、ElGamal 公開鍵暗号を用いた構成例を示す。

【0217】

この発明における第六の実施例では、アクセスチケット t は次の式 40 に基づいて生成されるデータである。

【0218】

【数 40】

$$(40) \quad t = X + F(p, e)$$

上式中の各記号は以下を表す。

【0219】

p は十分大きな素数である。

【0220】

ユーザ固有情報 e はユーザ毎に異なる数であり、ユーザを識別するために用いられる。

【0 2 2 1】

アクセスチケット秘密鍵 X は、法数 p のもとでの $E l G a m a l$ 暗号の秘密鍵であり、 Y を対応する公開鍵であるとする。即ち、式 4 1 を満たす。

【0 2 2 2】

【数 4 1】

$$(4\ 1) \quad Y = a^X \bmod p$$

ここで、 a は位数 p の有限体の乗法群の生成元、即ち、式 4 2 及び 4 3 を満たす。

【0 2 2 3】

【数 4 2】

$$(4\ 2) \quad a \neq 0$$

【0 2 2 4】

【数 4 3】

$$(4\ 3) \quad \min \{x > 0 \mid a^x = 1 \bmod p\} = p - 1$$

また、 Y をアクセスチケット公開鍵と呼ぶ。

【0 2 2 5】

二変数関数 $F(x, y)$ は関数値が衝突しにくい二変数関数であり、例えば、前述の一方方向ハッシュ関数 h を利用して、式 4 4 のように定めることができる。

【0 2 2 6】

【数 4 4】

$$(4\ 4) \quad F(x, y) = h(x \parallel y)$$

つぎに、図 2 3 および図 2 4 を参照して第六の実施例をさらに説明する。図 2 3 は第六の実施例の構成を示し、図 2 4 は第六の実施例におけるデータのフローを示している。図 2 3 において、証明データ検証装置 5 0 は、アクセスチケット公開鍵記憶部 5 0 1、乱数発生部 5 0 2、乱数記憶部 5 0 3、受信データ記憶部 5 0 5、乱数化部 5 2 1、認証用素データ記憶部 5 2 2、乱数効果除去部 5 2 3 および実行手段 3 1 0 を含んで構成されている。証明データ生成部 5 1 は、受信データ記憶部 5 1 1、第 1 演算部 5 1 2、アクセスチケット記憶部 5 1 3、第 2 演算部 5 1 4、ユーザ固有情報記憶部 5 1 5、証明データ生成部 5 1 6、および

指数生成部 530 を含んで構成されている。

【0227】

つぎに動作について説明する。

【0228】

1. ユーザがアクセスすることによって、証明データ検証装置 50 が起動される。

【0229】

2. 証明データ検証装置 50 は、認証用データの組 u 、 C と、アクセスチケット公開鍵記憶部 501 に記憶されている法数 p とを、証明データ生成装置 51 中の受信データ記憶部 511 に書き込む。

【0230】

認証用素データ記憶部 522 には、認証用素データとして u 、 C' が記憶されているが、それらは次の性質を満たす。

【0231】

u は、上記 a を法 p のもとで適当な乱数 z を指数としてべき乗した数であり、即ち、式 45 を満たす。

【0232】

【数 45】

$$(45) \quad u = a^z \bmod p$$

C' は、アクセスチケット公開鍵 Y を、法 p のもとで、上記乱数 z を指数としてべき乗した数と、適当なデータ K との積であり、式 46 を満たす。

【0233】

【数 46】

$$(46) \quad C' = Y^z K \bmod p$$

認証用データ C は、次のように生成される。

【0234】

証明データ検証装置 50 は、乱数発生部 502 によって、乱数 r をアクセスチケット公開鍵記憶部 501 に保持されている法数 p と互いに素になるように生成し、乱数記憶部 503 に記録する。

【0 2 3 5】

次いで、乱数化部 5 2 1 は、認証用素データ記憶部 5 2 2 に記憶されているデータ C' を取得して、式 4 7 の計算を行なう。

【0 2 3 6】

【数 4 7】

$$(4 7) \quad C = r C' \mod p$$

【0 2 3 7】

3. 証明データ生成装置 5 1 中の第 1 演算部 5 1 2 は、アクセスチケット記憶部 5 1 3 に記憶されているアクセスチケット t を取得し、受信データ記憶部 5 1 1 に書き込まれた法数 p のもとで式 4 8 を実行し中間情報 S を得る。

【0 2 3 8】

【数 4 8】

$$(4 8) \quad S = u^t \mod p$$

【0 2 3 9】

4. 証明データ生成装置 5 1 中の指数生成部 5 3 0 は、ユーザ固有情報記憶部 5 1 5 に記憶されているユーザの固有情報 e を取得し、式 4 9 の計算を実行する。

【0 2 4 0】

【数 4 9】

$$(4 9) \quad F(p, e)$$

【0 2 4 1】

5. 証明データ生成装置 5 1 中の第 2 演算部 5 1 4 は、指数生成部 5 3 0 で生成されたデータを用いて、式 5 0 の計算を実行し差分情報 S' を得る。

【0 2 4 2】

【数 5 0】

$$(5 0) \quad S' = u^{F(p, e)} \mod p$$

【0 2 4 3】

6. 証明データ生成装置 5 1 中の証明データ生成部 5 1 6 は、第 1 および第 2 演算部 5 1 2、5 1 4 から S および S' を得て、式 5 1 の計算を行ない R を得る。

【0 2 4 4】

【数 5 1】

$$(51) \quad R = S^{-1} S' C \bmod p$$

ただし、 S^{-1} は法 p のもとでの S の逆数、即ち、式 5 2 を満たす数を表す。

【0 2 4 5】

【数 5 2】

$$(52) \quad S S^{-1} \bmod p = 1$$

【0 2 4 6】

7. 証明データ生成装置 5 1 は R を証明データ検証装置 5 0 の受信データ記憶部 5 0 5 に返送する。

【0 2 4 7】

8. 証明データ検証装置 1 0 中の乱数効果除去部 5 2 3 は、乱数記憶部 5 0 3 中から先に生成した乱数 r を取り出し、式 5 3 の計算を行なう。

【0 2 4 8】

【数 5 3】

$$(53) \quad K' = r^{-1} R \bmod p$$

証明データ生成装置 5 1 において用いられるアクセスチケット t とユーザの固有情報 e の組合せが正しい場合に限り、計算の結果得られた K' と K が一致することに注意せよ。さて、上記の形態を直接実施した場合、次のような問題が生じる。即ち、同一の認証用素データ u , C' を、複数回のアクセス資格認証手続きに適用することにより、ユーザ固有情報やアクセスチケットなしに証明データ生成装置 1 1 の作用を模倣する装置を構成することが可能となる。まず、初回の認証手続きにおいて、証明データ検証装置 1 0 から発行される認証用素データ C と証明データ生成装置 1 1 が生成する証明データ R から、 $H = R C^{-1} \bmod p$ を計算する。模倣装置には、ユーザ固有情報及びアクセスチケットの代わりにこの H を記録しておく。証明データ検証装置 1 0 が発行する任意の認証用素データ (u, C) に対し、模倣装置が式 $R = H C \bmod p$ に従って証明データ R を生成し、証明データ検証装置 1 0 に返すようにすればよい。この攻撃に対処する方法として、認証用素データ記憶部 5 2 2 に認証用素データの組 u , C' を必要な数だけ記憶しておいて、認証手続きの都度使い捨てにすることが考えられる。

ここで、相異なる認証用素データでは、その生成のために用いられる乱数 z が互いに相違するようにする。

【0 2 4 9】

〔第七の実施例〕

この発明の第七の実施例においては、アクセス資格認証の特徴情報として E l G a m a l 署名の署名鍵を用いる構成例を述べる。

【0 2 5 0】

この発明における第七の実施例では、アクセスチケット t は式 5 4 に基づいて生成されるデータである。

【0 2 5 1】

〔数 5 4〕

$$(54) \quad t = X + F(p, e)$$

上式中の各記号は以下を表す。

【0 2 5 2】

p は十分大きな素数である。

【0 2 5 3】

ユーザ固有情報 e はユーザ毎に異なる数であり、ユーザを識別するために用いられる。

【0 2 5 4】

アクセスチケット秘密鍵 X は、法数 p のもとでの E l G a m a l 署名の署名鍵であり、 Y を対応する公開鍵であるとする。即ち、式 5 5 を満たす。

【0 2 5 5】

〔数 5 5〕

$$(55) \quad Y = a^X \bmod p$$

ここで、 a は位数 p の有限体の乗法群の生成元、即ち、式 5 6 及び 5 7 を満たす。

【0 2 5 6】

〔数 5 6〕

$$(56) \quad a \neq 0$$

【0257】

【数57】

$$(57) \quad \min \{x > 0 \mid a^x = 1 \pmod{p}\} = p - 1$$

また、Yをアクセスチケット公開鍵と呼ぶ。

【0258】

二変数関数 $F(x, y)$ は関数値が衝突しにくい二変数関数であり、例えば、前述の一方方向ハッシュ関数 h を利用して、式58のように定めることができる。

【0259】

【数58】

$$(58) \quad F(x, y) = h(x \parallel y)$$

つぎに図25および図26を参照してさらに第七の実施例について説明する。図25は第七の実施例の構成を示し、図26は第七の実施例におけるデータのフローを示している。図25において、証明データ検証装置60は、アクセスチケット公開鍵記憶部601、乱数発生部602、乱数記憶部603、受信データ記憶部605、検証部606、実行部607およびエラー処理部608を含んで構成されている。また、証明データ生成装置61は、受信データ記憶部611、乱数発生部612、第1演算部613、第2演算部614、アクセスチケット記憶部615、およびユーザ固有情報記憶部616を含んで構成されている。つぎに動作について説明する。

【0260】

1. ユーザがアクセスすることによって、証明データ検証装置60が起動される。

【0261】

2. 証明データ検証装置60は、認証用データCと、アクセスチケット公開鍵記憶部601に記憶されている法数 p と、生成元 a とを、証明データ生成装置61中の受信データ記憶部611に書き込む。認証用データCは、次のように生成される。

【0262】

証明データ検証装置60は、乱数発生部602によって、乱数 r をアクセスチ

ケット公開鍵記憶部 6 0 1 に保持されている法数 p と互いに素になるように生成し、前記 r を乱数記憶部 6 0 3 に記録するとともに、認証用データ C とする ($C = r$)。

【0 2 6 3】

3. 証明データ生成装置 6 1 中の乱数生成部 6 1 2 は、法数 $p - 1$ と互いに素であるような乱数 k を生成する。

【0 2 6 4】

第 1 演算部 6 1 3 は、前記乱数 k と、受信データ記憶部 6 1 1 に書き込まれた法数 p と、生成元 a とから、第一の証明データ R を式 5 9 に従って計算する。

【0 2 6 5】

【数 5 9】

$$(59) \quad R = a^k \bmod p$$

第 2 演算部 6 1 4 は、アクセスチケット記憶部 6 1 5 に記憶されているアクセスチケット t と、ユーザ固有情報記憶部 6 1 6 に記憶されているユーザ固有情報 e と、前記乱数 k と、前記第一の証明データ R と、受信データ記憶部 6 1 1 に書き込まれた認証用データ C と、法数 p とから、第二の証明データ S を式 6 0 に従って計算する。

【0 2 6 6】

【数 6 0】

$$(60) \quad S = (C - R(t - F(p, e))) k^{-1} \bmod p - 1$$

【0 2 6 7】

4. 証明データ生成装置 6 1 は第一および第二の証明データである R 及び S を証明データ検証装置 6 0 の受信データ記憶部 6 0 5 に返送する。

【0 2 6 8】

5. 証明データ検証装置 6 0 中の検証部 6 0 6 は、乱数記憶部 6 0 3 に記憶されている乱数 $r (= C)$ と、アクセスチケット公開鍵記憶部 6 0 1 に記憶されている Y 及び p とを取り出し、式 6 1 によって、証明データ R 及び S を検証する。

【0 2 6 9】

【数 6 1】

$$(61) \quad a^r = Y^R R^S \bmod p$$

【0270】

〔第八の実施例〕

この発明の第八の実施例では、アクセスチケットの生成方法について述べる。

【0271】

第一乃至第七の実施例におけるアクセスチケットの生成には、秘密数に基づく計算が必要である。従って、アクセスチケットの生成は、計算に用いる秘密数が漏洩したり、計算の中間結果が露呈する心配のない安全な装置で実行される必要がある。

【0272】

このような安全な装置を構成するための最も容易な方法は、アクセスチケット発行サービスをユーザに提供するサーバを、ユーザが使用するPCあるいはワークステーションから独立な計算機上に構築することである。サーバは、ユーザからの要求に応じてアクセスチケットを生成する。サーバの構成に当たっては、外部からの侵入を遮断するように構成することにより、秘密数およびアクセスチケットの計算手順を守る。

【0273】

例えば、アクセスチケット発行サーバを、施錠され、出入りが厳重に管理される個室内の計算機上に構成することにより、外部からの侵入を遮断することが可能となる。

【0274】

また、ユーザの利便を向上させるために、前記アクセスチケット発行サーバをネットワークに接続し、ユーザからのアクセスチケット発行要求をネットワークを介して受け取り、生成したアクセスチケットをやはりネットワークを介してユーザに配送するように構成することも可能である。

【0275】

このように、アクセスチケット発行サーバをネットワークに接続する場合には、ファイアウォール技術 (D. Brent Chapman & Elizabeth D. Zwicky, Building Internet Fire

w a l l s, O' R e i l l y & A s s o c i a t e s, I n c. あるいは邦訳、ファイアウォール構築、オライリー・ジャパンを参照)を利用して、ネットワークを介した外部からの侵入に対しても十分に安全性が保たれるよう構築される必要がある。

【 0 2 7 6 】

第一乃至第七の実施例におけるアクセスチケットは、その正当な使用者（アクセスチケットを計算する際に用いたユーザ固有情報 e を保持するユーザ）以外には利用できない形式で生成されている。

【 0 2 7 7 】

第一乃至第七の実施例におけるアクセスチケットは、更に厳密な安全基準のもとに生成されている。即ち、不正なアクセスを試みるユーザが、本人向けあるいは他人向けを問わず、任意個数のアクセスチケットを集めたとしても、そこから、別のアクセスチケットを偽造したり、第一乃至第五の実施例で述べた証明データ生成装置の動作を模倣する装置を構成することは不可能である。

【 0 2 7 8 】

上記のようなアクセスチケットの安全性から、アクセスチケット発行サーバが生成したアクセスチケットを、電子メールのような比較的安全性の低い配送手段を利用してユーザに配送することも可能となる。

【 0 2 7 9 】

[第九の実施例]

この実施例では、第一乃至第七の実施例とは異なるユーザの固有情報およびアクセスチケットの構成法を述べる。この構成方法の特徴は、アクセスチケットの生成に秘密情報を必要としない点にある。

【 0 2 8 0 】

従って、アクセスチケット生成に際して、第八の実施例で述べたような、外部からの侵入に対して安全に構築されたアクセスチケット発行サーバは必要ない。ユーザは、所有する P C あるいはワークステーション上で動作するプログラムによって自由にアクセスチケットを生成することができる。プログラム中には、秘密の定数や秘密の手続きは存在せず、プログラムを解析したとしても不正アクセ

スを可能とするいかなる情報も取り出すことはできない。

【0281】

ユーザUの固有情報はRSA公開鍵ペアの個人鍵dである。このユーザの固有情報に対応する公開鍵を (e_U, n_U) とする。即ち、異なる2つの大きい素数 p_U と q_U に対し $n_U = p_U q_U$ であり、 d_U 及び e_U は関係式62を満たすように決定された整数である。

【0282】

【数62】

$$\begin{aligned} 1 &\leq d_U \leq (p_U - 1)(q_U - 1) \\ (62) \quad 1 &\leq e_U \leq (p_U - 1)(q_U - 1) \\ e_U d_U &\equiv 1 \pmod{(p_U - 1)(q_U - 1)} \end{aligned}$$

ここで、 n_U は全てのユーザに共有される定数N以上であるという条件を付け加える。

【0283】

ユーザUへのアクセスチケットは以下のように構成される。

【0284】

RSA公開鍵ペアの公開鍵 (E, n) をアクセスチケットの公開鍵とし、該公開鍵と対をなす秘密鍵をDとする。ここで $n < N$ である。 n の素因数分解を $n = pq$ とする時、関係式63が成り立つ。

【0285】

【数63】

$$\begin{aligned} (63) \quad 1 &\leq D < (p - 1)(q - 1) \\ DE &\equiv 1 \pmod{(p - 1)(q - 1)} \end{aligned}$$

アクセスチケット t_U は式64で定義される。

【0286】

【数64】

$$(64) \quad t_U = D^{e_U} \pmod{n_U}$$

この実施例におけるアクセス資格認証の特徴情報は、前記RSA公開鍵ペアの個人鍵Dである。

【0287】

第一乃至第七の実施例の場合と同様、この実施例における証明データ生成装置 11 は、アクセス資格認証の特徴情報を知りえること、即ち、与えられた認証用データに対応して、正しい証明データを計算し得ることを、証明データ検証装置 10 との通信を介して証明する。

【0288】

この実施例の特徴は、アクセス資格認証の特徴情報である D を暗号化して得られるデータがアクセスチケットであり、ユーザの固有情報がこの暗号化を解くための唯一の復号鍵である点にある。更にいえば、ユーザの固有情報を RSA 公開鍵暗号の個人鍵としている所から、対応する公開鍵を知りえる何人でもアクセスチケットを生成しえる点にある。以下に、本実施例における作用を図 27 を参照して述べる。

【0289】

1. 証明データ検証装置 10 は、認証用データ C および法数 n を証明データ生成装置 10 の受信データ記憶部 711 に書き込む。

【0290】

2. 証明データ生成装置 11 の復号鍵生成部 712 は、ユーザ固有情報記憶部 713 中に記憶されたユーザの固有情報 d_U と、アクセスチケット記憶部 715 中に記憶されたアクセスチケット t_U を取得し、式 65 に基づき D' を計算する。

【0291】

【数 65】

$$(65) \quad D' = t_U^{d_U} \bmod n_U$$

【0292】

3. 証明データ生成部 714 は、復号鍵生成部 712 によって生成された前記 D' と、受信データ記憶部 711 に記憶されている認証用データ C を入力として式 66 の計算を行ない、R を求める。証明データ生成部 714 は、計算結果を返信データとして証明データ検証装置に送信する。

【0293】

【数 66】

$$(66) \quad R = C^{D'} \bmod n$$

【0294】

4. 証明データ検証装置は、証明データRの正当性を検証する。

【0295】

アクセスチケット $t_U = D^{e_U} \bmod n_U$ におけるアクセスチケットの秘密鍵Dは、ユーザUに対しても秘密に保たなければならないので、上記証明データ生成装置11の装置構成のうち、ユーザ固有情報記憶部713、復号鍵生成部712および証明データ生成部714は耐タンパー特性を有する防御手段760中に封入される。

【0296】

第1乃至第七の実施例の場合と同様、証明データ生成装置11によってユーザの第一の固有情報とアクセスチケットの正しい組合せが用いられた場合に限り、証明データ生成装置によって生成される証明データRは、証明データ検証装置によって正しく検証される。

【0297】

【第十の実施例】

この発明の第十の実施例は、証明データ生成装置における証明データの計算に公開鍵暗号(RSA暗号)の代わりに対称鍵暗号が利用され、アクセスチケットが、前記対称鍵暗号の復号鍵(暗号化鍵と同一)Dをユーザ固有情報であるRSA公開鍵ペアの個人鍵に対応する公開鍵(e_U, n_U)で暗号化して得られるデータである点を除いては、第九の実施例とほぼ同じである。

【0298】

即ち、対称鍵暗号の暗号化関数をEncrypt(鍵, 平文)(出力は暗号文)、復号関数をDecrypt(鍵, 暗号文)(出力は平文)と表す時、プロテクトされた証明データCは式67で定義される。

【0299】

【数67】

$$(67) \quad C = \text{Encrypt}(D, K)$$

更に、アクセスチケット t_U は式68で定義される。

【0300】

【数68】

$$(68) \quad t_U = D^{e_U} \bmod n_U$$

以下、証明データ生成装置の装置構成および作用を図27に基づいて説明する。

【0301】

1. 証明データ検証装置10は、認証用データCを証明データ生成装置10の受信データ記憶部711に書き込む。

【0302】

2. 証明データ生成装置11の復号鍵生成部712は、ユーザ固有情報記憶部713中に記憶されたユーザの固有情報 d_U と、アクセスチケット記憶部715中に記憶されたアクセスチケット t_U を取得し、式71により D' を計算する。計算結果は証明データ生成部714に出力される。

【0303】

【数69】

$$(69) \quad D' = t_U^{d_U} \bmod n_U$$

【0304】

3. 証明データ生成部714は、復号鍵生成部712から得た D' と、受信データ記憶部711に記憶されている認証用データCを入力として式70の計算を行ない、Rを求める。計算結果は、返信データとして証明データ検証装置10に送信される。

【0305】

【数70】

$$(70) \quad R = \text{Decrypt}(D', C)$$

【0306】

4. 証明データ検証装置11中はRの検証を行い、正規の処理を続行するか、エラー処理を実行するかを決定する。

【0307】

【実施例の効果】

以上の説明から明らかなように、ユーザのPCあるいはワークステーション上で実行されるアプリケーションプログラムへのアクセス制御（実行制御）を目的として、上記の実施例を実施した場合、次に述べる効果を提供することができる。

【0308】

1. ユーザはユーザ固有情報を固有にただ一つ保持すればよい。

【0309】

2. データ記憶装置においてユーザ固有情報と無関係な方法でプロテクト処理を施す。

【0310】

3. データ記憶装置へのアクセスを許可されたユーザにはアクセスチケットが発行され、該ユーザは自らのユーザ固有情報とアクセスチケットを保持することによってのみデータ記憶装置へのアクセスが可能となる。

【0311】

4. アクセスチケットは、正規の持ち主ではないユーザがそれを保持していたとしても、それによってデータ記憶装置へのアクセスが可能にならないような方法で、安全に生成される。

【0312】

これらの特徴により、ユーザ固有情報を内蔵したハードウェアをユーザに配布する場合でも、配布は各ユーザ毎に一回で済み、また、データ記憶装置を保護する者は、だれによってアクセスされるかに関わりなく、一つのデータ記憶装置の保護処理を一通りの方法で行なえばよいこととなる。

【0313】

上述の実施例によれば、データ記憶装置へのアクセスにはアクセスチケットが必要となるが、アクセスチケットは正規のユーザにのみ利用可能な安全なデジタル情報であるため、ネットワーク等を介して簡便にユーザに配送することが出来る。

【0314】

また、ユーザはアクセス対象のデータ記憶装置ごとにアクセスチケットを取り

替える必要があるが、前述のようにアクセスチケットはデジタル情報であるため取り替え操作は計算機中のプログラムによって容易に行なうことができる。

【0315】

なお、本発明は上述の実施例に限定されるものではなくその趣旨を逸脱しない範囲で種々変更が可能である。例えば、上述実施例では、証明データを生成する際に認証用補助情報（アクセスチケット）を用いるようにしたが、認証用補助情報を検証時に用いるようにしてもよい。この構成を図28に示す。なお、図28において図3と対応する箇所に対応する符号を付して詳細な説明は省略する。

【0316】

また、上述ではアプリケーションのユーザのアクセス資格を認証してデータ記憶装置へのアクセスを制御するようにしたが、個々のアプリケーション自体のアクセス資格を認証してデータ記憶装置へのアクセスを制御する構成としてもよい。このアプリケーションとしては例えばJ A V Aアプレットとしてサーバから取り出して実行するものでもよい。またアプリケーションサーバが提供するアプリケーションとしてもよい。このようにするとアプリケーションの管理を行ってセキュリティを実現できる。

【0317】

また、上述実施例ではデータ記憶装置は追記型の記録媒体を有するものとしたが、追記型の記録媒体と通常の更新書きこみ可能な記録媒体とを併せ持つようにしてもよい。この場合、アクセスログ等、改竄等の発見に必要なデータ等、特定のデータを除いてデータを更新書きこみ可能な記録媒体に記録する。なお、追記型記録媒体はバックアップ用に用いられるのではなく通常のハードディスク装置と同様に補助記憶装置として用いられることに留意されたい。

【0318】

また、アクセス資格の認証機能を用いない場合でも、アクセスログ等特定のデータを除いてデータを更新書きこみ可能な記録媒体に記録し、特定のデータは追記型の記録媒体に記録することにより、改竄等に対処でき、また更新書き込みによる記録媒体の有効利用を図ることができる。

【0319】

【発明の効果】

以上説明したように、この発明によれば、アプリケーションプログラムがデータ記憶装置に記憶されたファイルにアクセスする際に、アクセス資格認証機能付きデータ記憶装置によりアプリケーションプログラムのユーザのアクセス資格が認証され、正しい資格を有することが確認された場合に限って、データ記憶装置中のファイルへのアクセスが認められる。

【0320】

また、証明用補助データ（アクセスチケット）を導入することにより、アクセス資格認証の特徴情報とアプリケーションプログラムのユーザの固有情報とを独立させることができ、従って、アクセス資格認証機能付きデータ記憶装置側も、アプリケーションプログラムのユーザ側も1つの特徴情報・固有情報を準備しておけば済む。アクセスチケットは、特定のアプリケーションプログラムのユーザの固有情報とアクセス資格認証の特徴情報とに基づいて計算されるデータであり、またアプリケーションプログラムのユーザの固有情報を知らずにアクセスチケットからアクセス資格認証の特徴情報を計算することは少なくとも計算量的に不可能である。そしてアプリケーションプログラムのユーザの固有情報とアクセスチケットとの正しい組合せ、即ち、アプリケーションプログラムのユーザの固有情報と該アプリケーションプログラムのユーザの固有情報に基づいて計算されたアクセスチケットの組合せが入力された場合に限って、正しい証明用データが計算される。従って、アプリケーションプログラムはあらかじめアプリケーションプログラムのユーザの固有情報を保有し、アクセス資格認証機能付きデータ記憶装置はアプリケーションプログラムが所持するアプリケーションプログラムのユーザの固有情報とは独立にアクセス資格認証の特徴情報を用意し、アクセスチケットをアプリケーションプログラムのユーザの固有情報とアクセス資格認証の特徴情報とに応じて作成し、配布することにより、実行制御等のアプリケーションプログラムのユーザのアクセス資格の認証を行なうことができる。

【0321】

また、記録媒体の少なくとも一部を追記型の光記憶媒体とすることにより、第1段階の壁を通り抜けてきた不正アクセス、及び内なる敵からの不正アクセスに

よる破壊、改竄からなる攻撃を防止することができる。

【図面の簡単な説明】

【図 1】 この発明の原理的な構成例を示すブロック図である。

【図 2】 上述構成例のクライアント側の具体例を説明する図である。

【図 3】 上述構成例の要部を説明するブロック図である。

【図 4】 第一の実施例の証明データ検証装置及び証明データ生成装置の構成を示すブロック図である。

【図 5】 第一の実施例の動作を説明するフロー図である。

【図 6】 第二の実施例の証明データ検証装置及び証明データ生成装置の構成を示すブロック図である。

【図 7】 第二の実施例の証明データ検証装置の動作を説明するフロー図である。

【図 8】 第二の実施例の証明データ検証装置の実行部の構成例を示すブロック図である。

【図 9】 図 8 の実行部の構成例の動作を説明するフロー図である。

【図 1 0】 第二の実施例の証明データ検証装置の実行部の他の構成例を示すブロック図である。

【図 1 1】 図 1 0 の実行部の構成例の動作を説明するフロー図である。

【図 1 2】 第二の実施例の証明データ検証装置の実行部の他の構成例を示すブロック図である。

【図 1 3】 図 1 2 の実行部の構成例の動作を説明するフロー図である。

【図 1 4】 第二の実施例の証明データ検証装置の実行部の他の構成例を示すブロック図である。

【図 1 5】 図 1 4 の実行部の構成例の動作を説明するフロー図である。

【図 1 6】 この発明の第三の実施例の証明データ生成装置の構成を示すブロック図である。

【図 1 7】 第三の実施例の証明データ生成装置の動作を説明するフロー図である。

【図 1 8】 この発明の第四の実施例の構成例を示すブロック図である。

【図 1 9】 この発明の第四の実施例の他の構成例を示すブロック図である。

【図 2 0】 図 1 8 の動作を説明するフロー図である。

【図 2 1】 この発明の第五の実施例の構成を示すブロック図である。

【図 2 2】 第五の実施例のデータ検証装置の動作を説明するフロー図である。

【図 2 3】 この発明の第六の実施例の構成を示すブロック図である。

【図 2 4】 第六の実施例の動作を説明するフロー図である。

【図 2 5】 この発明の第七の実施例の構成を示すブロック図である。

【図 2 6】 第七の実施例の動作を説明するフロー図である。認証プロトコルを説明する図である。

【図 2 7】 第九の実施例および第十の実施例のアクセスチケットを用いた認証を説明するブロック図である。

【図 2 8】 図 B の構成の変形例を説明するブロック図である。

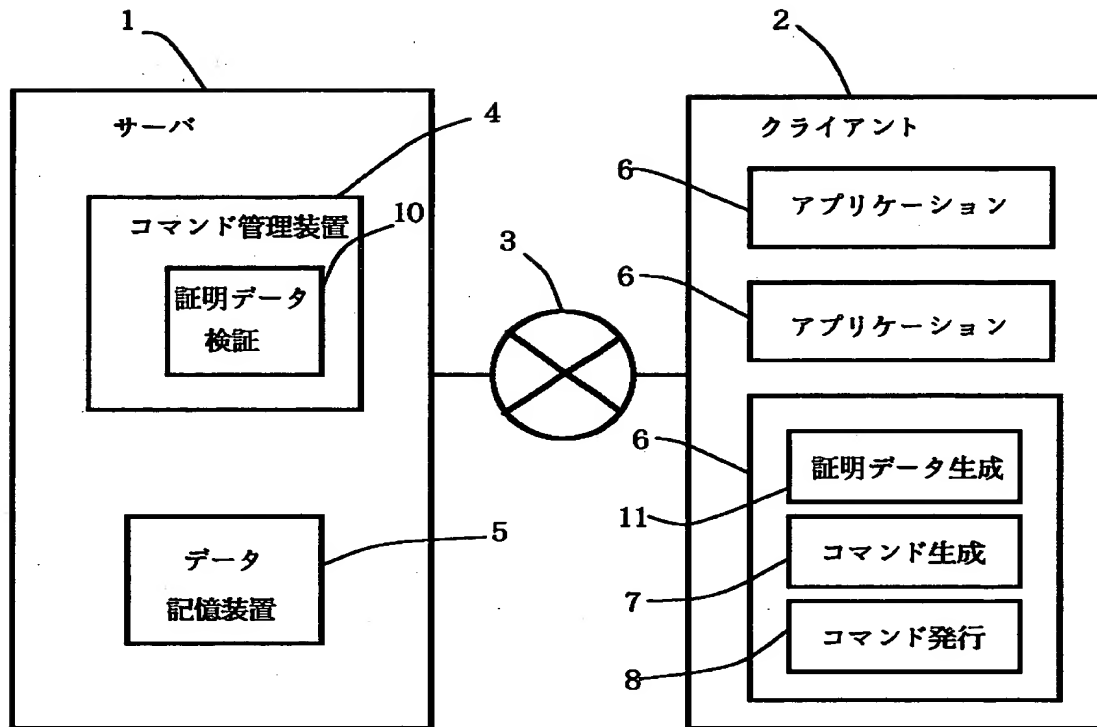
【符号の説明】

- 1 サーバ
- 2 クライアント
- 3 ネットワーク
- 4 コマンド管理装置
- 5 データ記憶装置
- 6 アプリケーション
- 7 コマンド生成装置
- 8 コマンド発行装置
- 1 0 証明データ検証装置
- 1 1 証明データ生成装置
- 1 2 アクセスチケット生成装置
- 1 3 アクセスチケット
- 1 4 アクセス資格認証の特徴情報
- 1 5 検証ルーチン

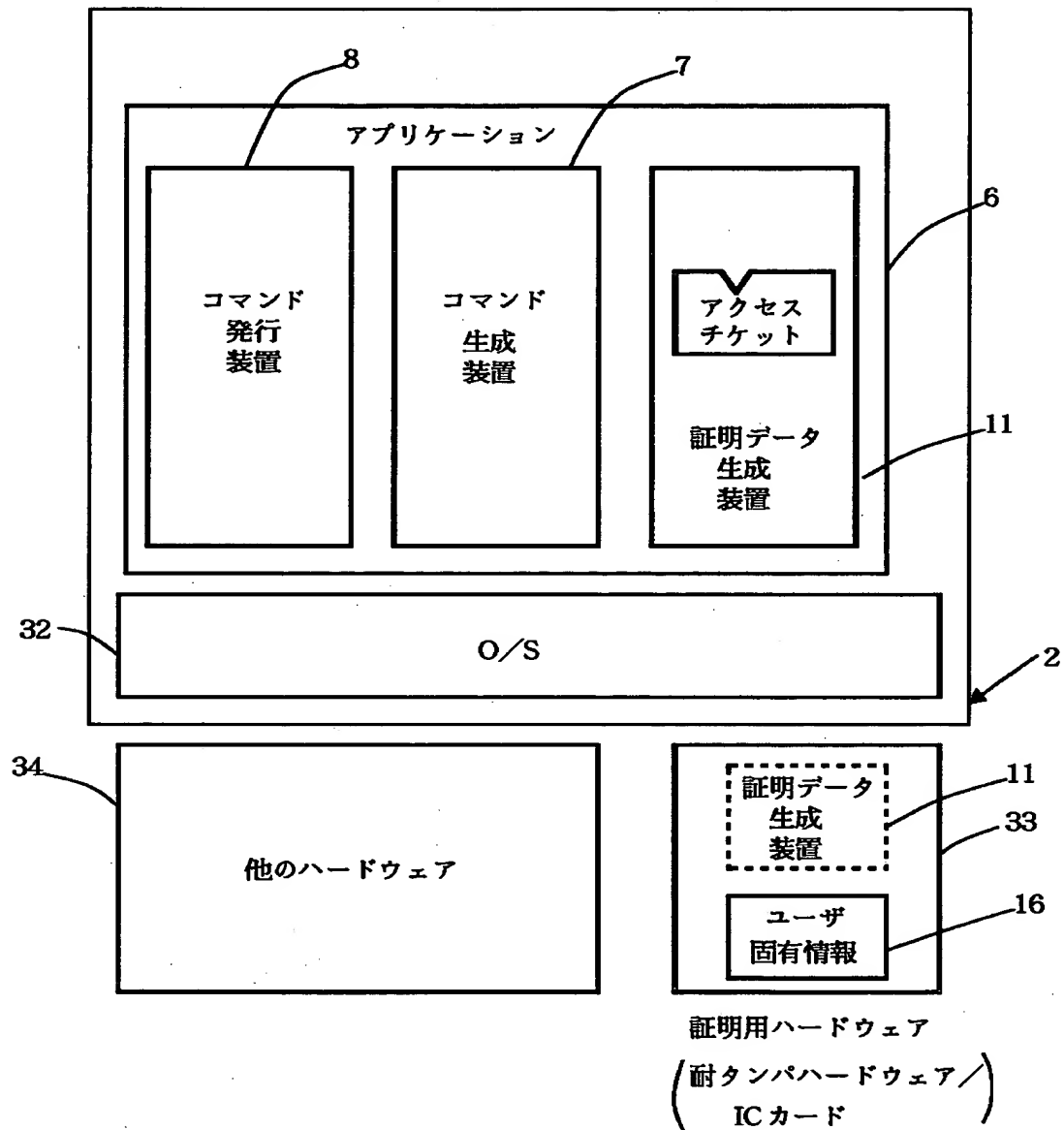
- 1 6 ユーザ固有情報
- 1 7 証明データ生成プログラム
- 2 0 トークン（防護手段）
- 1 0 1 アクセスチケット公開鍵記憶部 1 0 1
- 1 0 2 乱数発生部
- 1 0 3 乱数記憶部
- 1 0 5 受信データ記憶部
- 1 0 6 検証部
- 1 0 7 実行部
- 1 0 8 エラー処理部
- 1 1 1 受信データ記憶部
- 1 1 2 第 1 演算部
- 1 1 3 アクセスチケット記憶部
- 1 1 4 第 2 演算部
- 1 1 5 ユーザ固有情報記憶部
- 1 1 6 証明データ生成部

【書類名】 図面

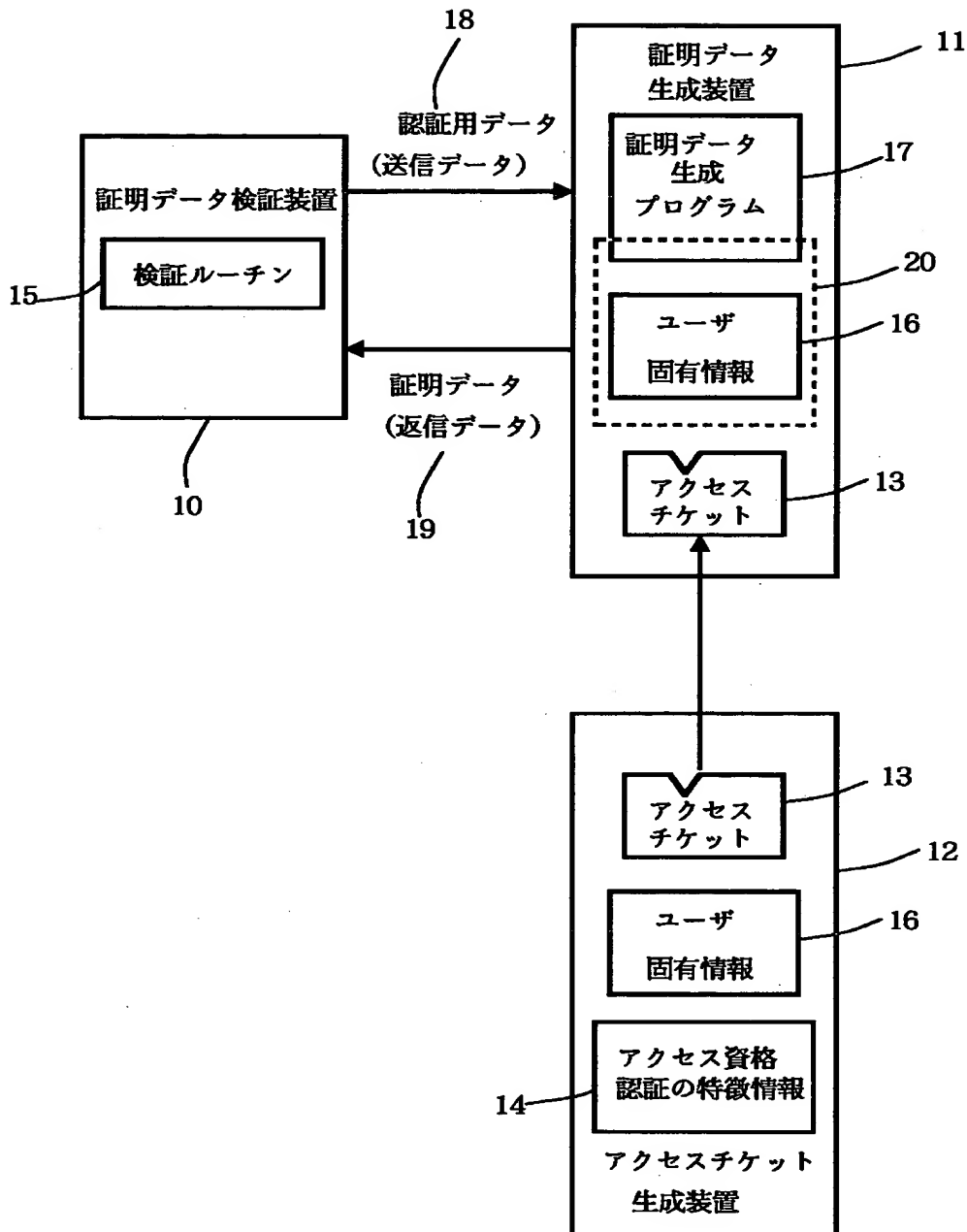
【図 1】



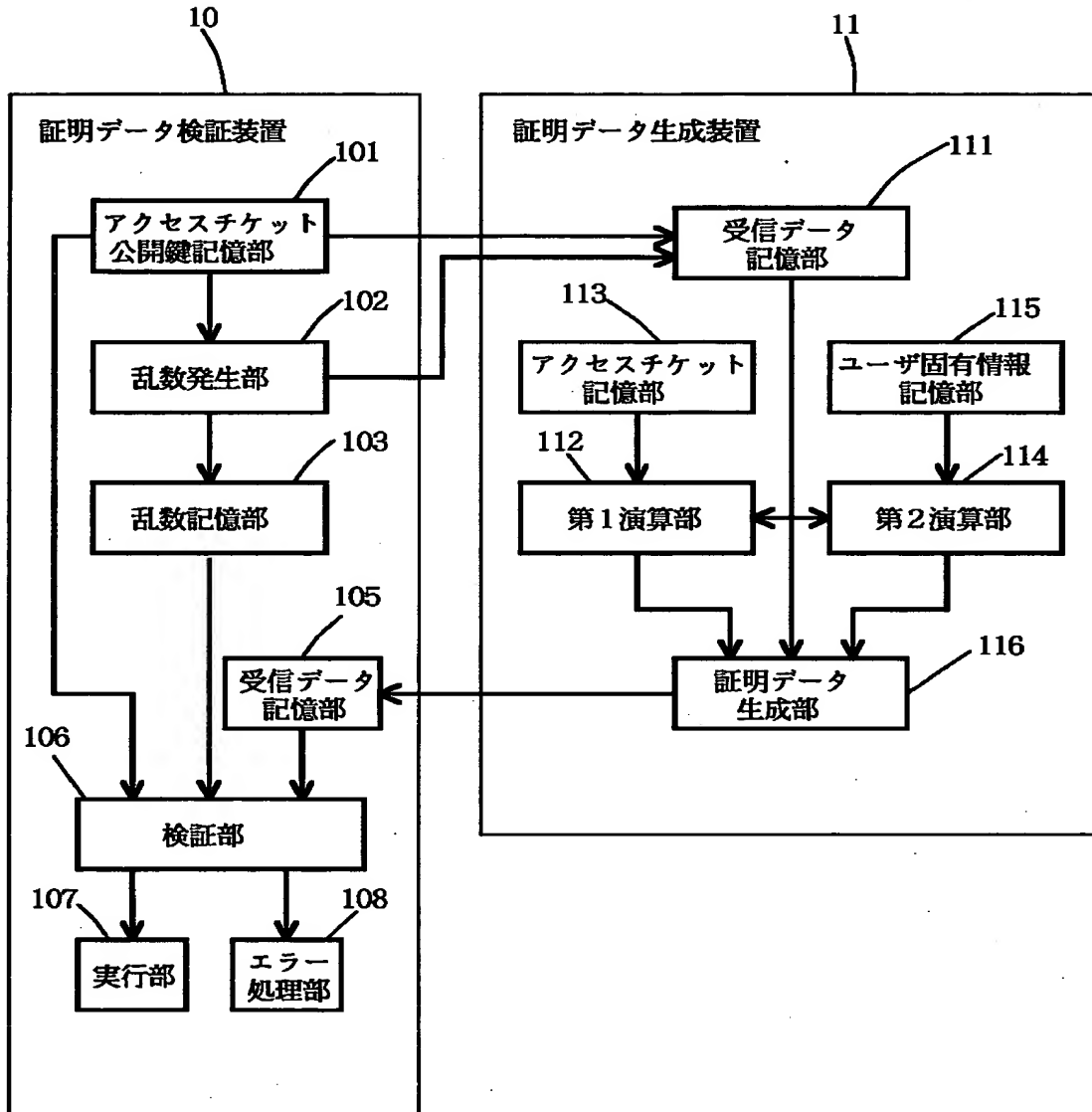
【図 2】



【図 3】

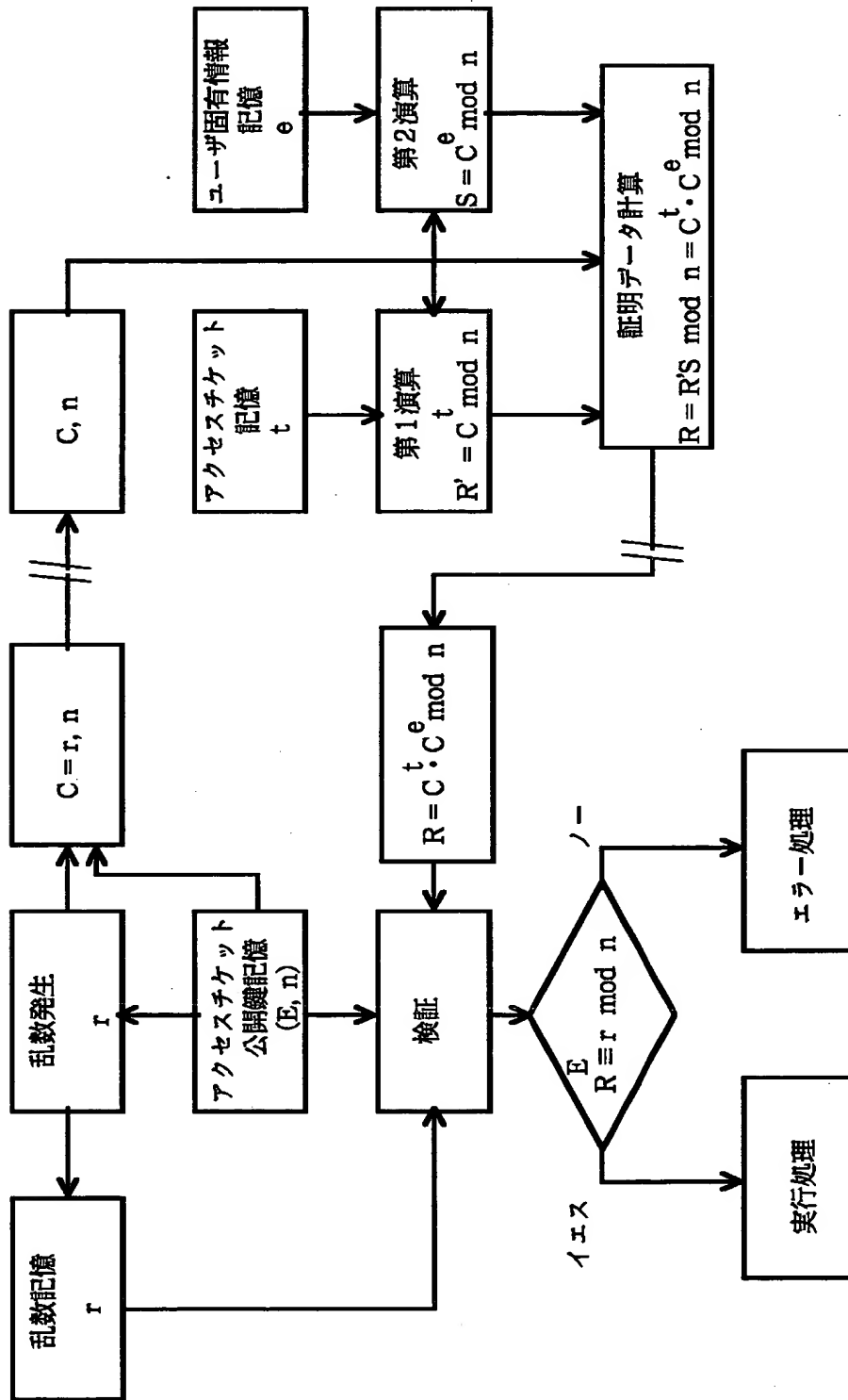


【図 4】

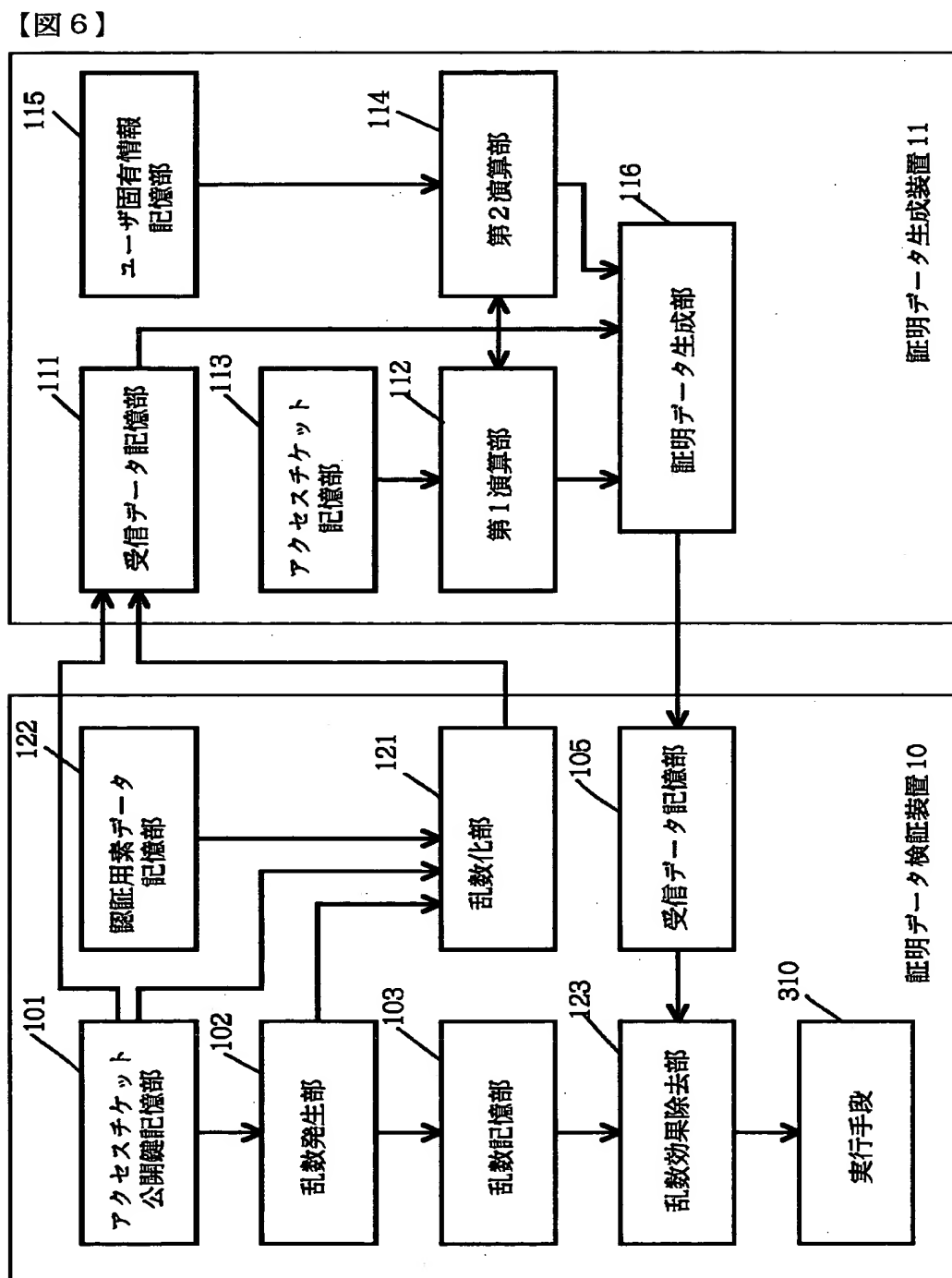


第一の実施例

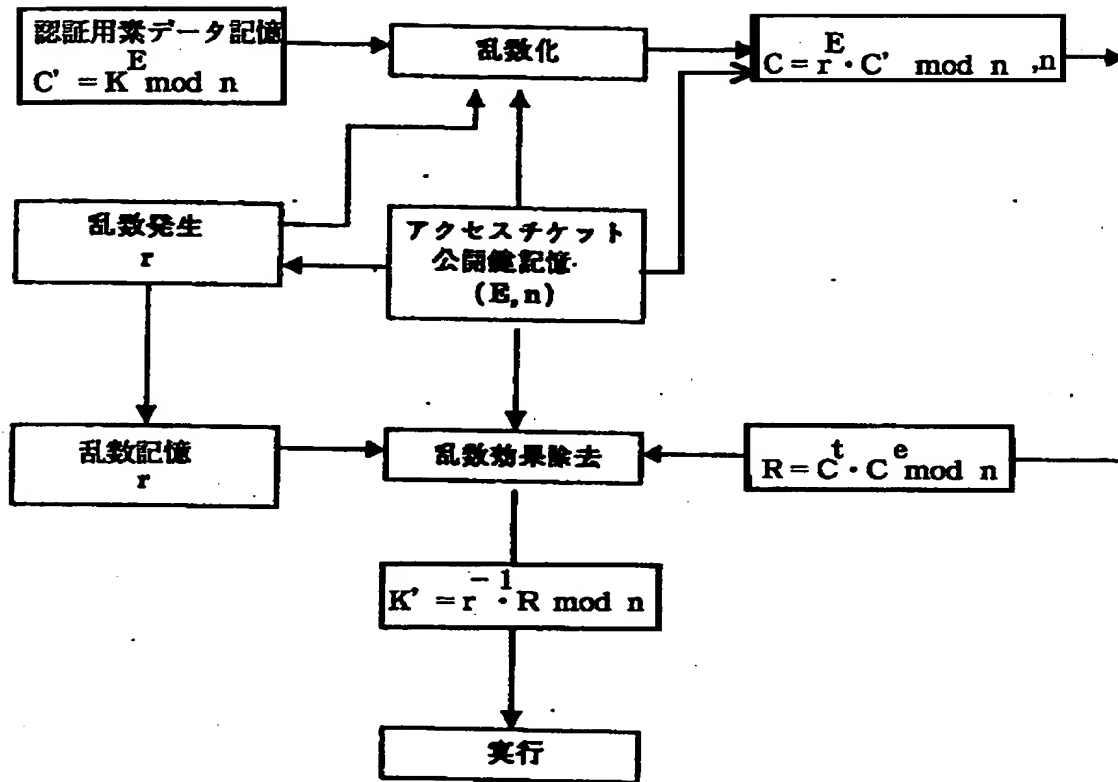
【図 5】



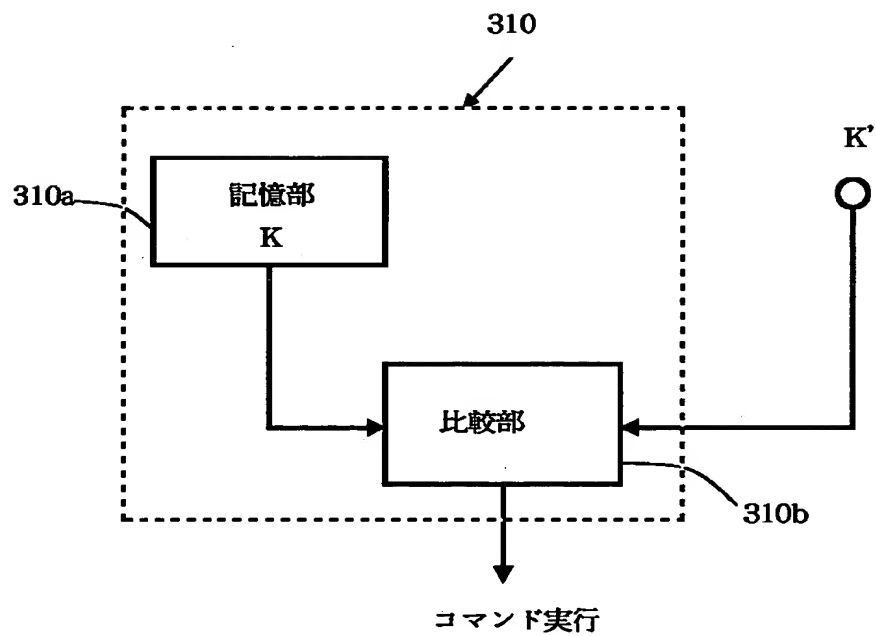
第二の実施例



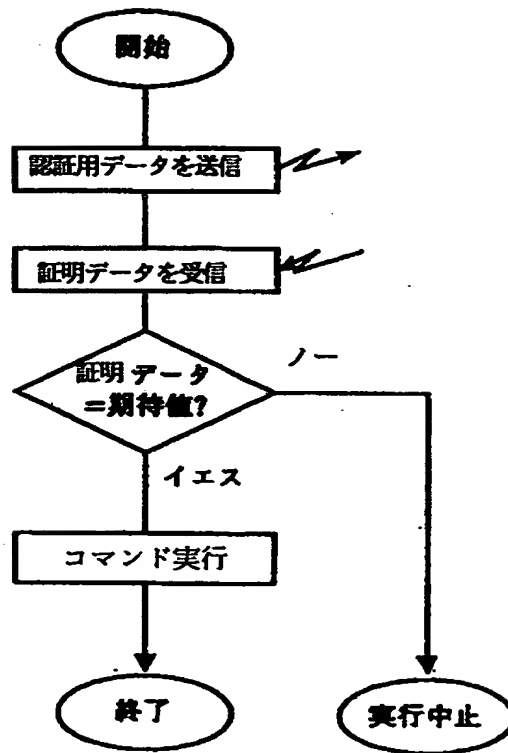
【図 7】



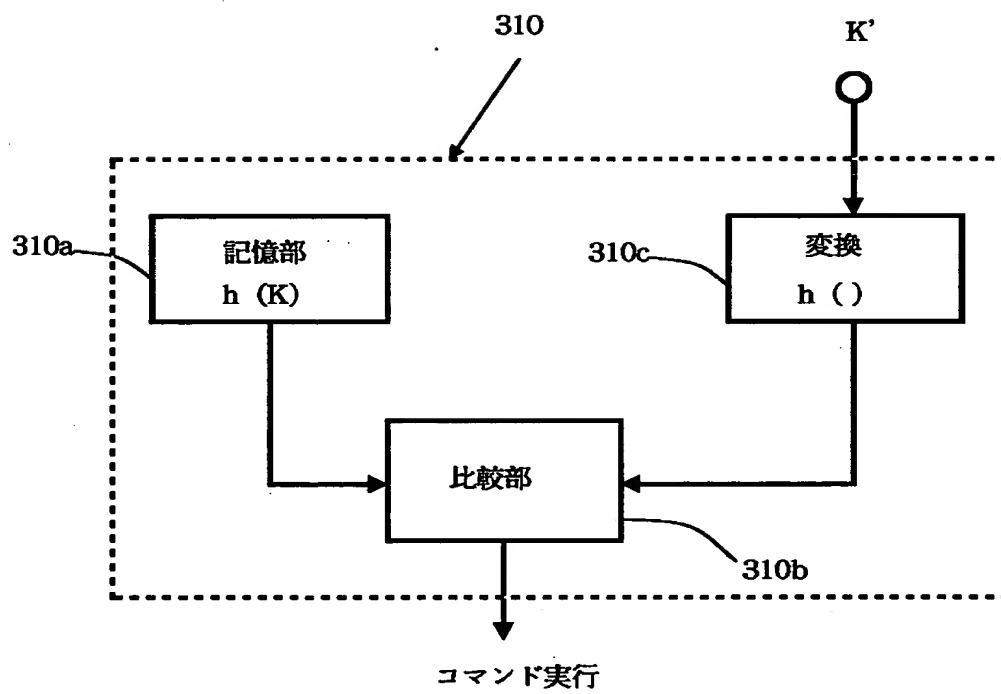
【図 8】



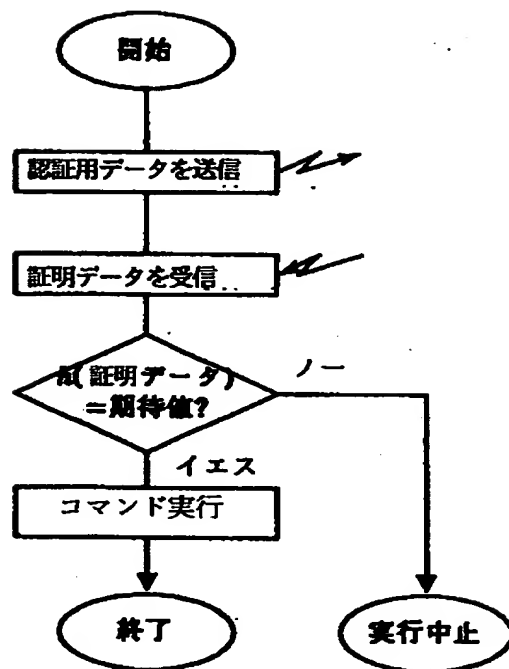
【図 9】



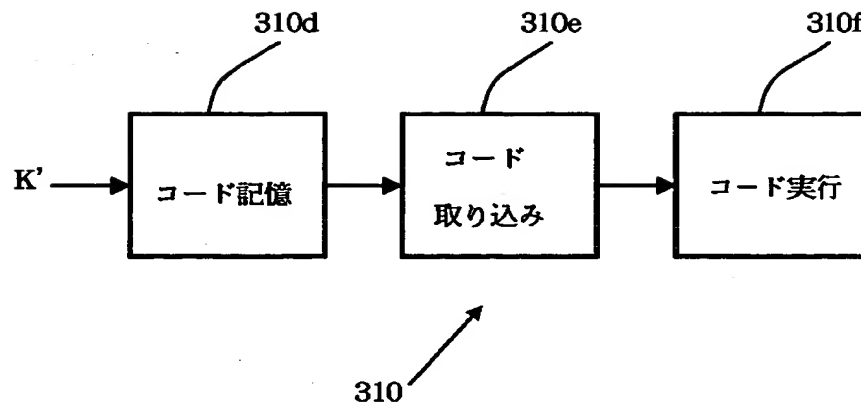
【図 1 0】



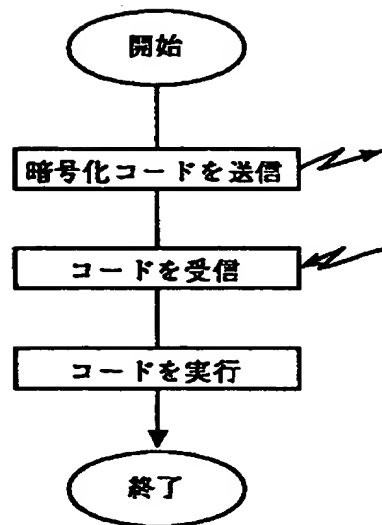
【図 1 1】



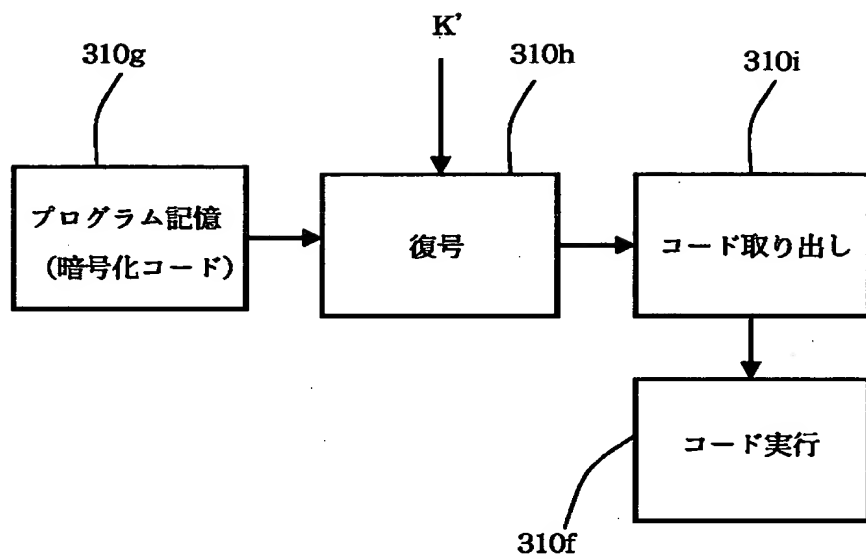
【図 1 2】



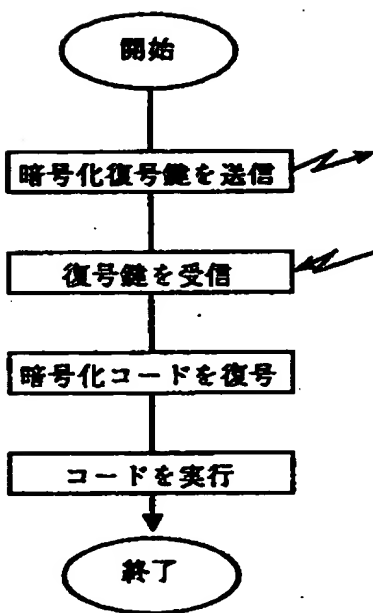
【図 1 3】



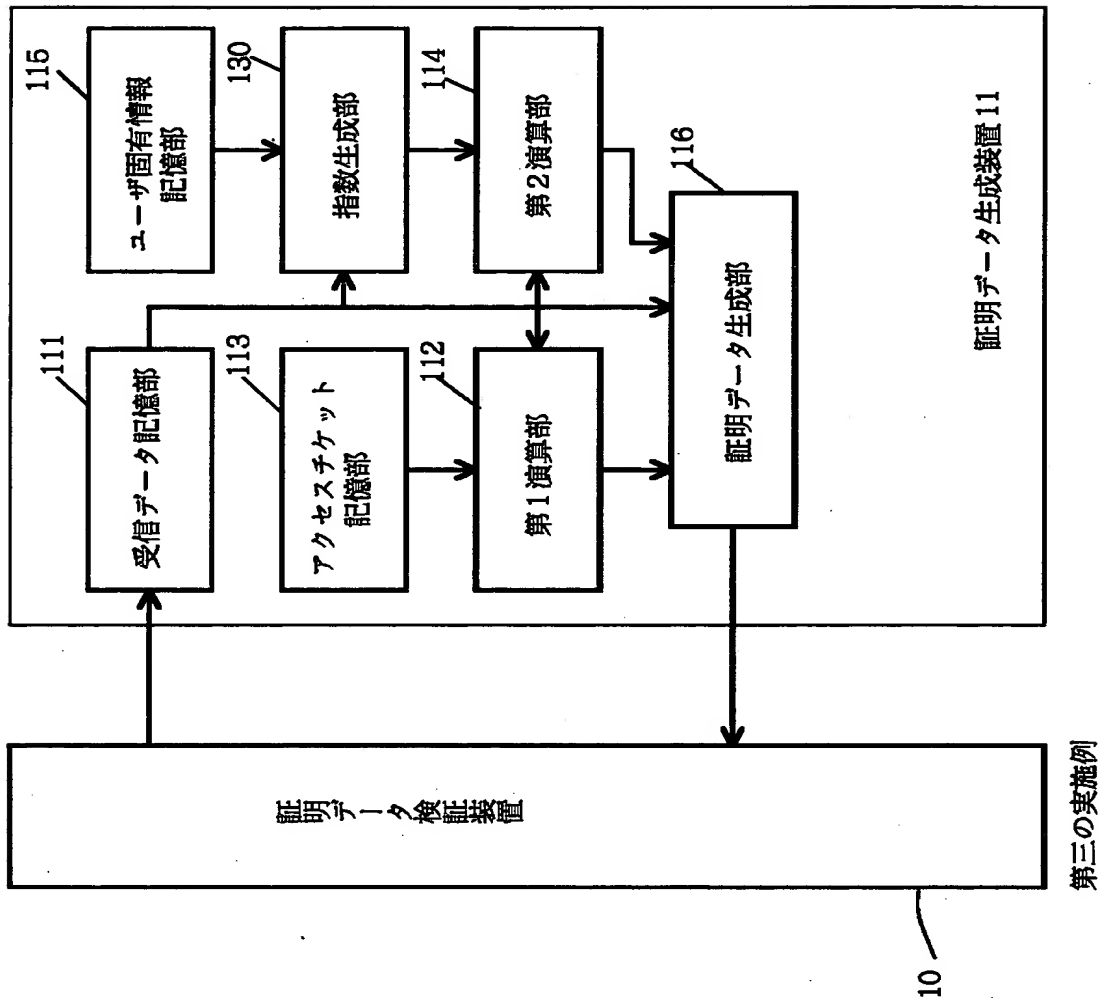
【図 1 4】



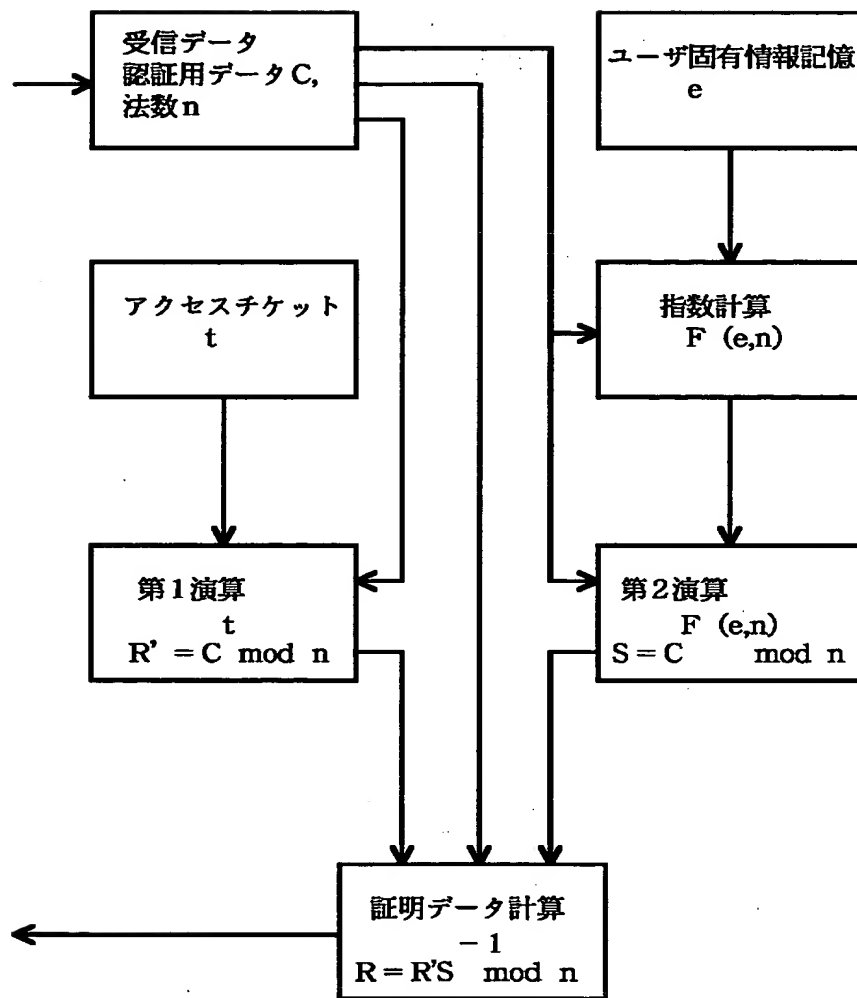
【図 1 5】



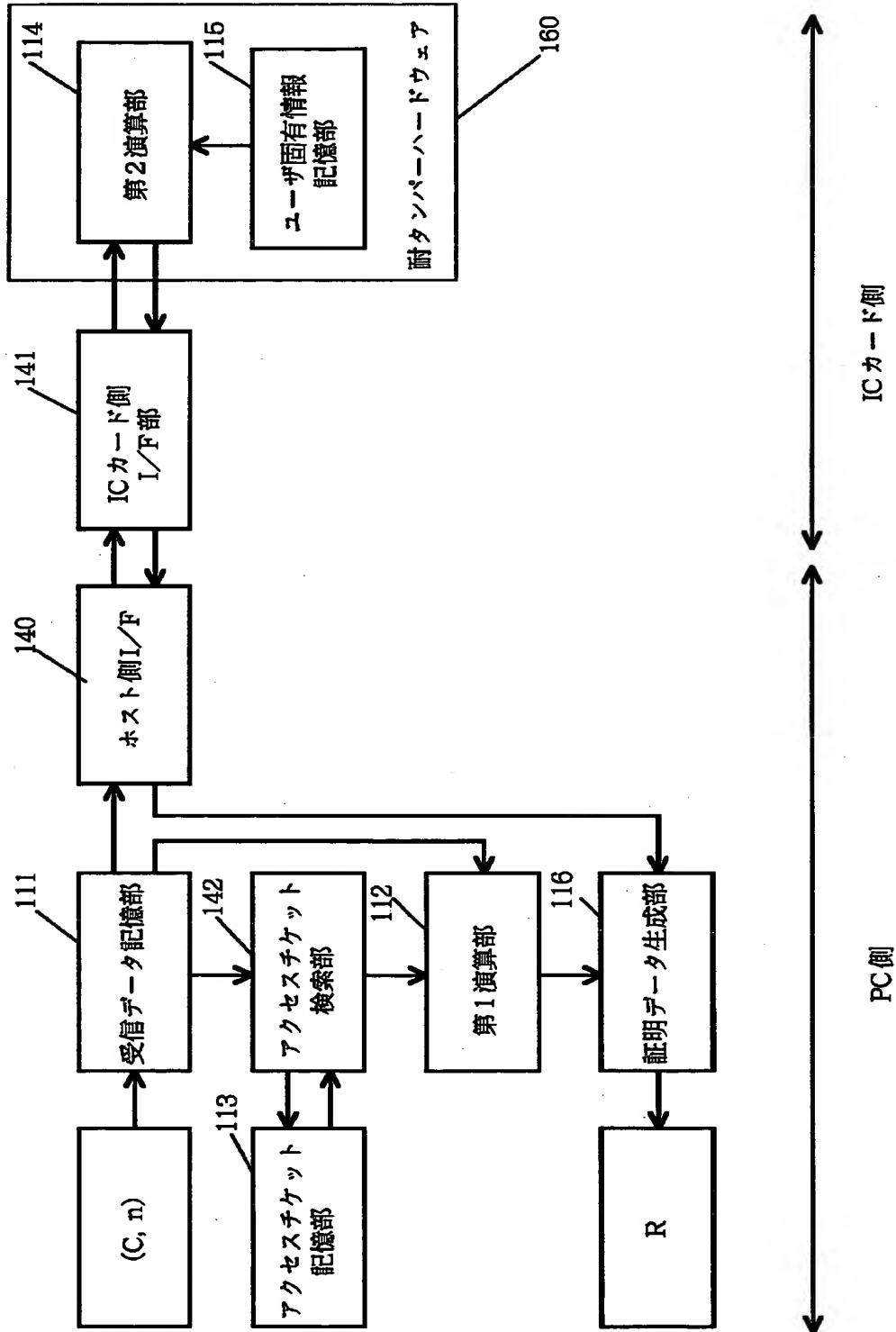
【図 1 6】



【図 1 7】

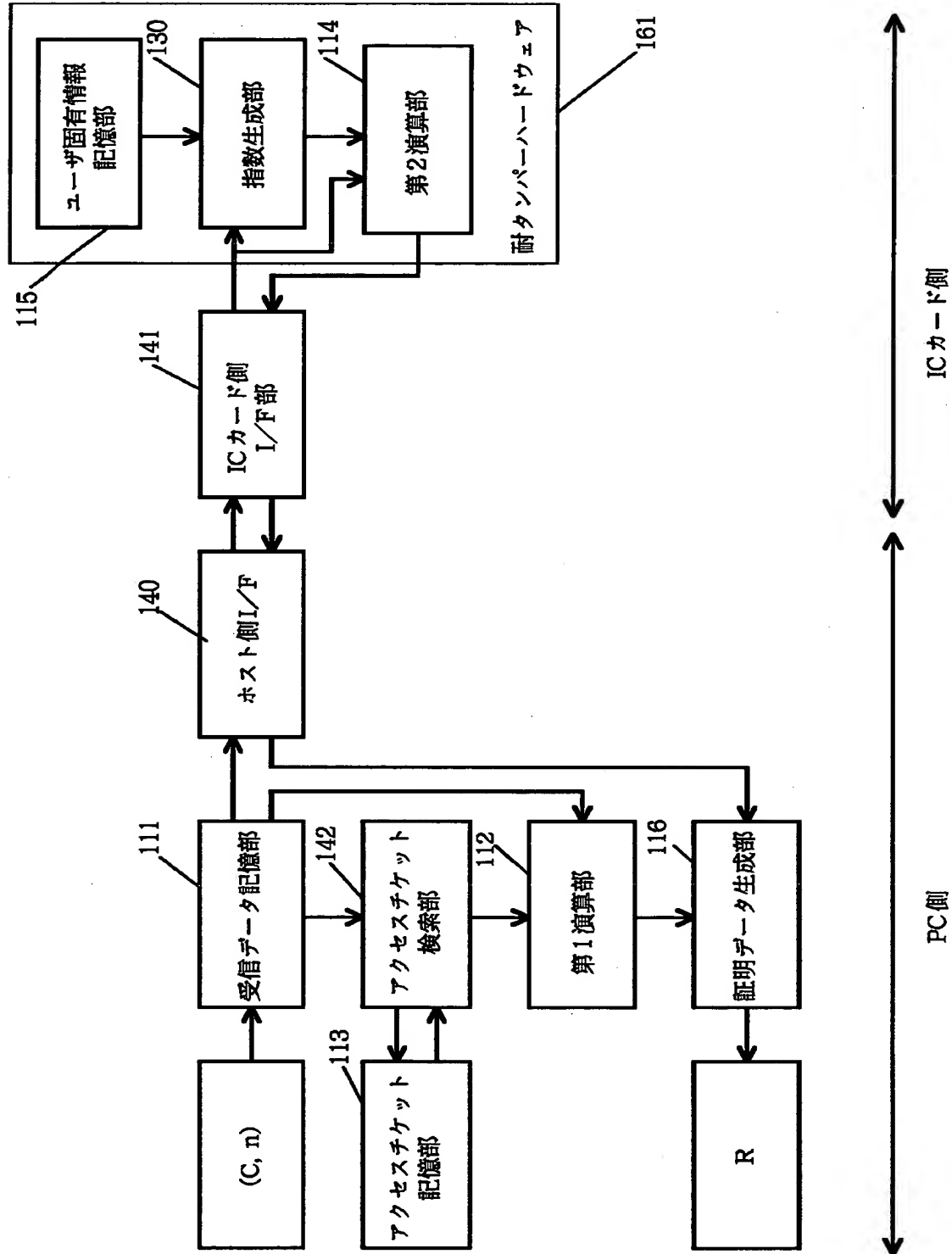


【図 1 8】

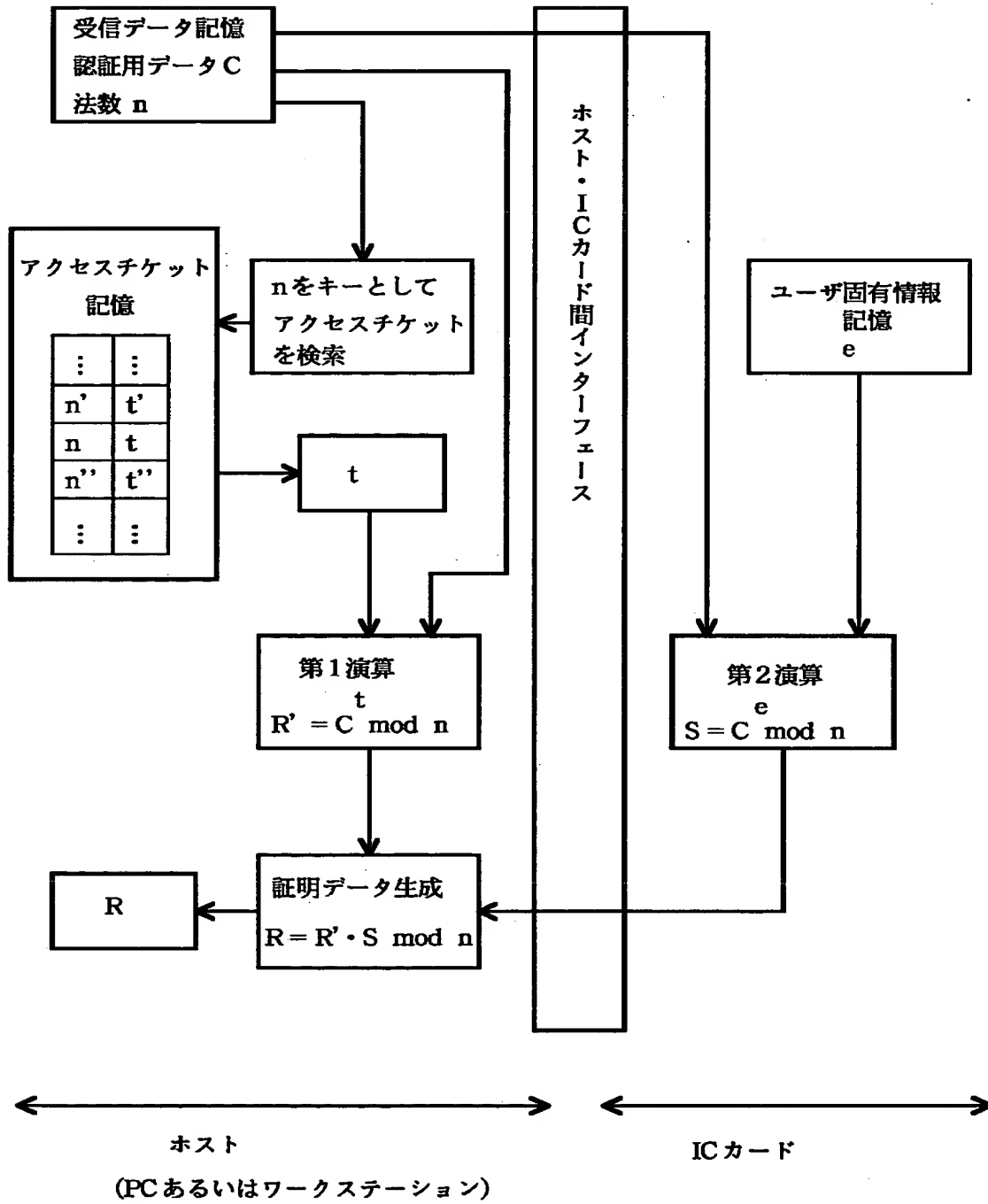


第四の実施例

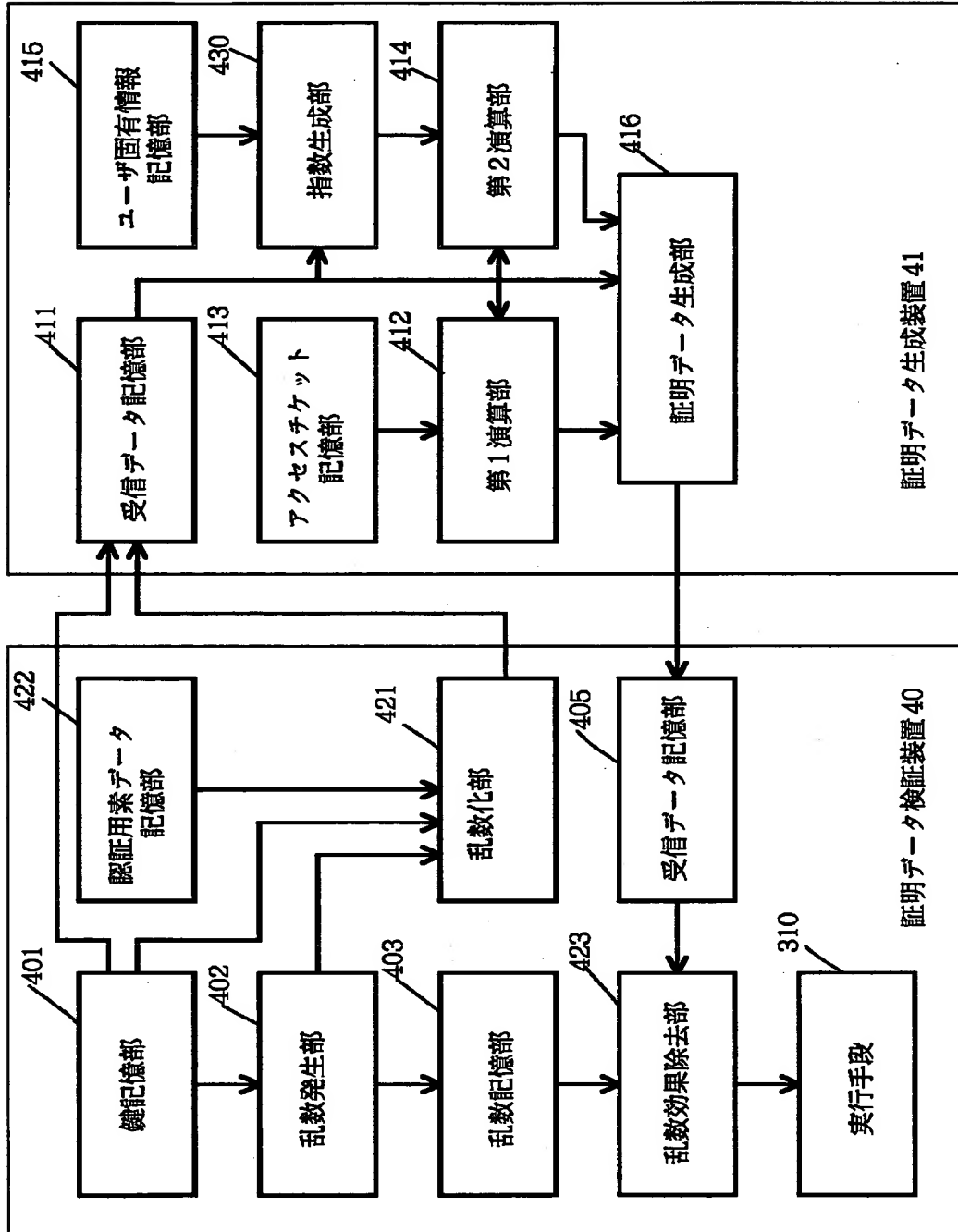
【図 1 9】



【図 2 0】

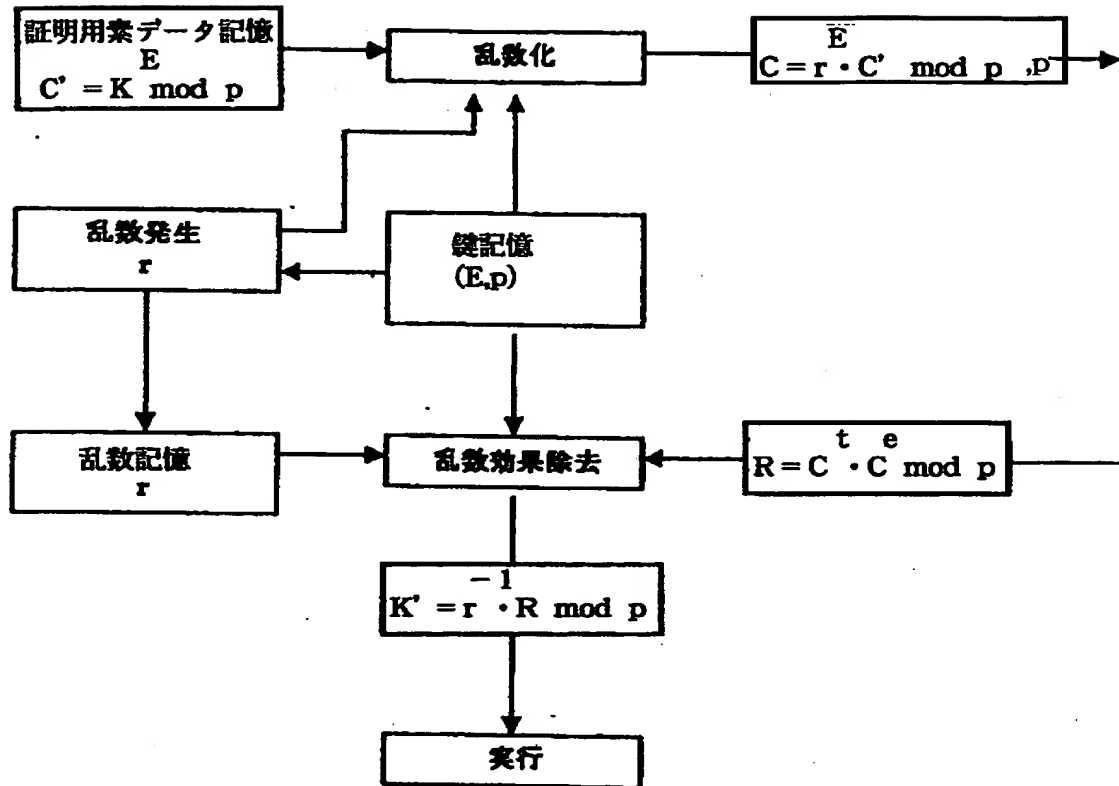


【図 2 1】



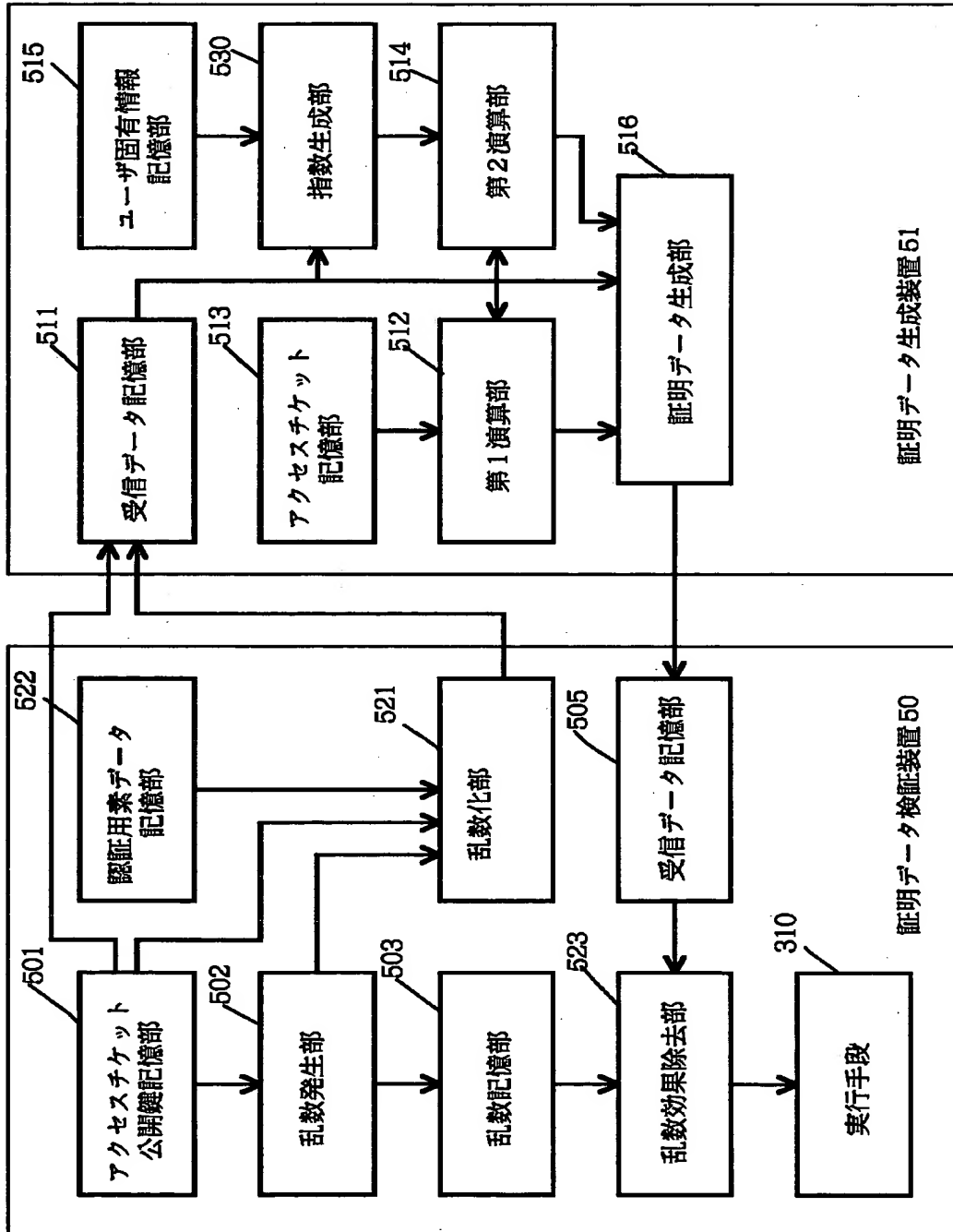
第五の実施例

【図 2 2】

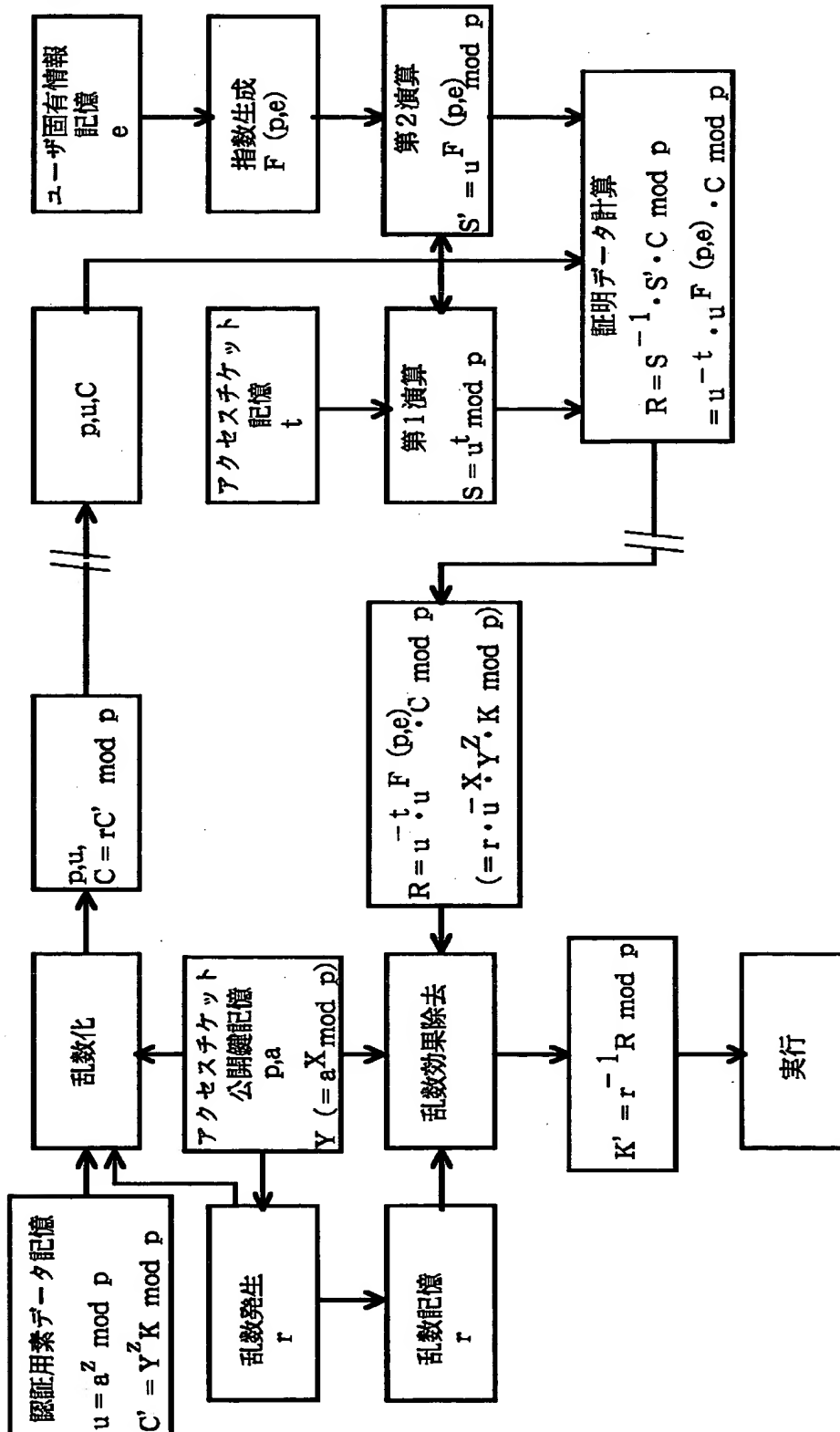


【図 2 3】

第六の実施例

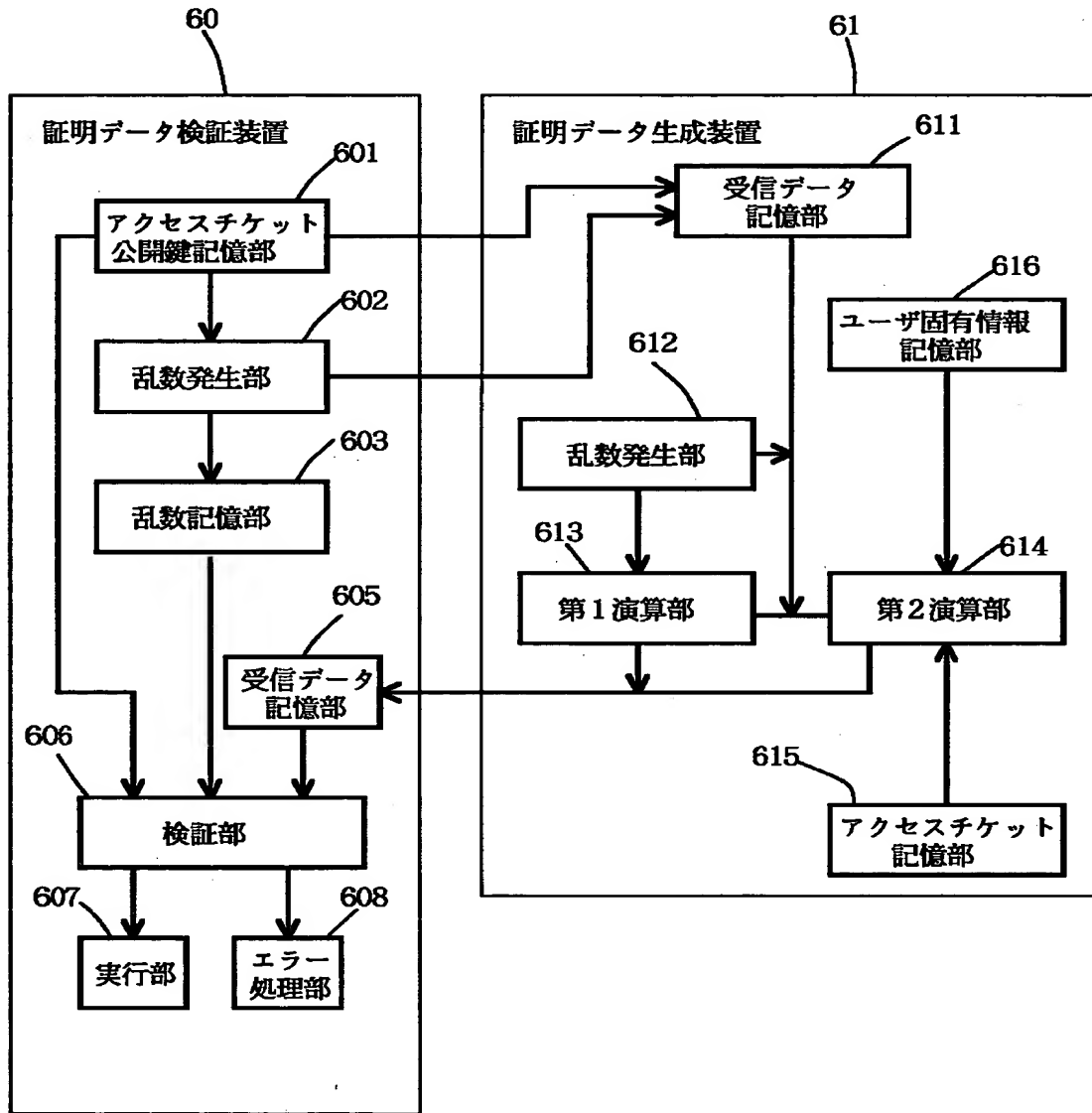


【図 2 4】

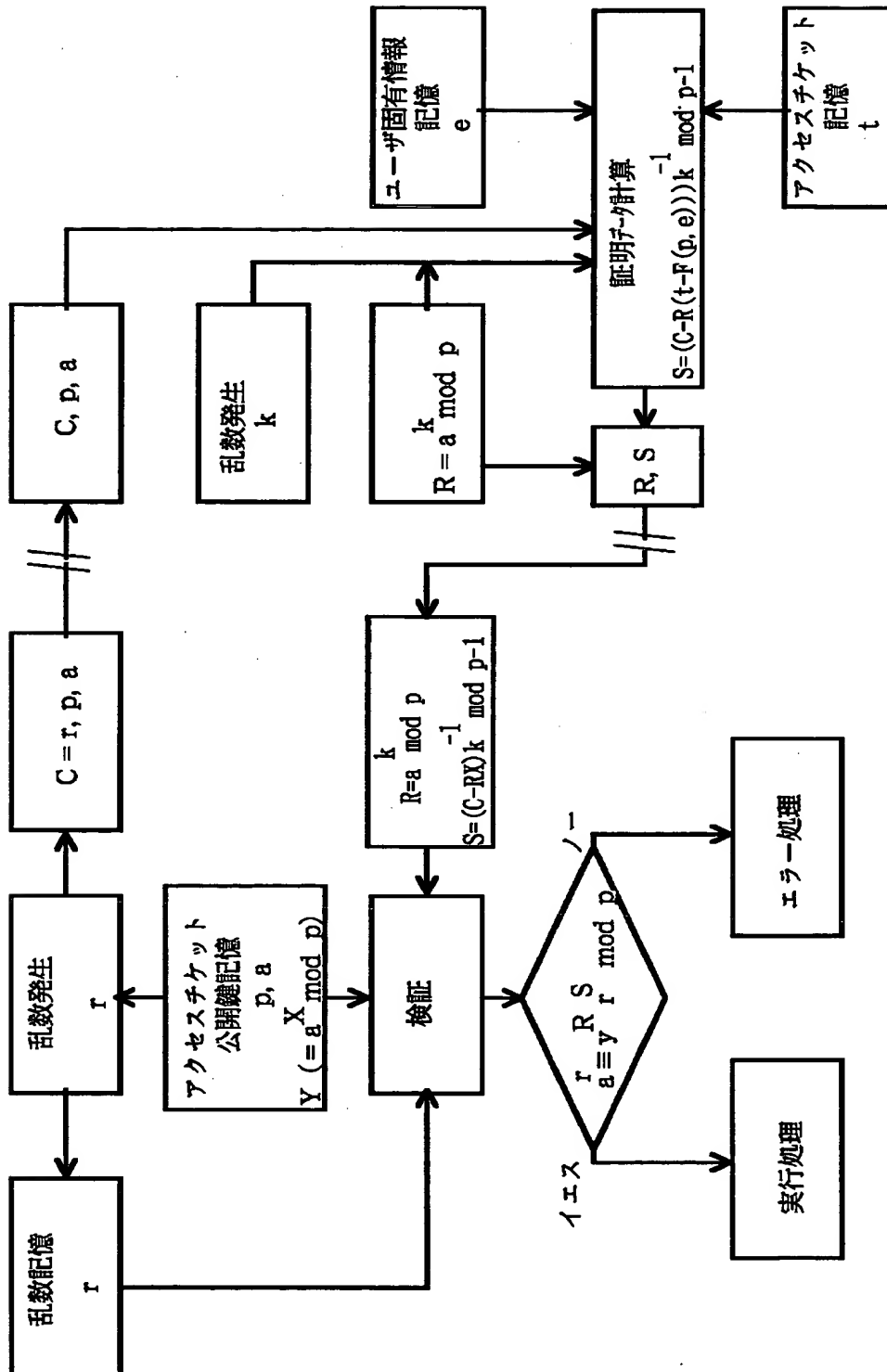


【図 2 5】

第七の実施例

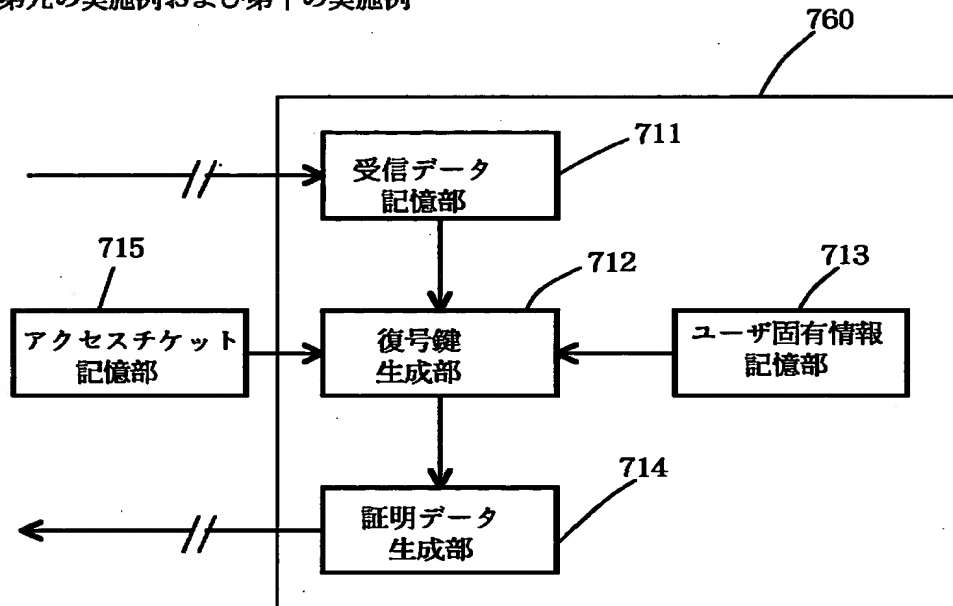


【図 2 6】

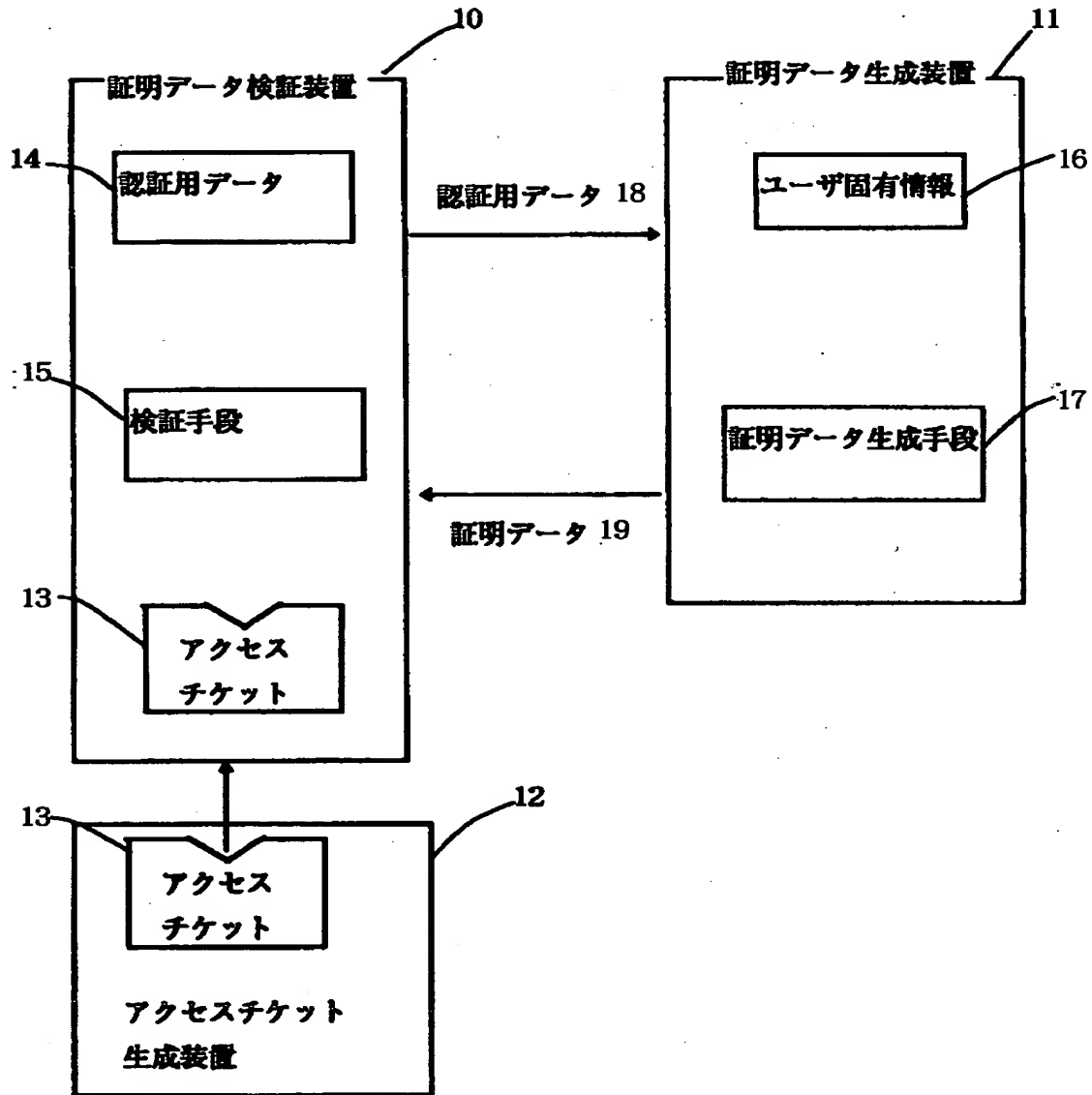


【図 2 7】

第九の実施例および第十の実施例



【図 2 8】



【書類名】 要約書

【要約】

【課題】 データ記憶装置へのアクセスを柔軟に制御する。

【解決手段】 クライアント 2 上のアプリケーション 6 は、証明データ生成装置 1 1、コマンド生成装置 7、コマンド発行装置 8 を具備している。クライアント 2 のアプリケーション 6 からコマンドおよび証明データがサーバ 1 に送られ、サーバ 1 のコマンド管理装置 4 がこれを受け取り、証明データ検証装置 1 0 が証明データに基づいてアプリケーション 6 のユーザのアクセス資格を検証し、検証が成功したら、コマンドに基づいてデータ記憶装置 5 をアクセス可能にする。データ記憶装置 5 は、慣用的に用いられるハードディスクドライブの代わりに用いられ、相変化方式光記憶媒体や相分離方式光記憶媒体を具備して追記型の記録を行う。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 4 9 6]

1. 変更年月日	1 9 9 6 年 5 月 2 9 日
[変更理由]	住所変更
住 所	東京都港区赤坂二丁目 1 7 番 2 2 号
氏 名	富士ゼロックス株式会社